DUDLEY KNOX LIBRARY
NAVAL POSTGRADUATE SCHOOL
MONTEREY CA 93943-5101

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

A STUDY OF COMPUTER SECURITY POLICIES FOR THE INDONESIAN NAVY

by

Antonius Herusutopo

June 1993

Thesis Co-Advisor: Prof.Timothy J.Shimeall
Thesis Co-Advisor: Prof. Roger Stemp

Approved for public release; distribution is unlimited.

UNCLASSIFIED

CURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited
. DECLASSIFICATION/DOWNGRADING SCHEDULE	
PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)
. NAME OF PERFORMING ORGANIZATION omputer Science Dept. aval Postgraduate School — 6b. OFFICE SYMBOL (if applicable) CS	7a. NAME OF MONITORING ORGANIZATION Naval Postgraduate School
. ADDRESS (City, State, and ZIP Code) Ionterey, CA 93943-5000	7b. ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000
. NAME OF FUNDING/SPONSORING ORGANIZATION — 8b. OFFICE SYMBOL (if applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS: PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO

. TITLE (Include Security Classification)
STUDYOF COMPUTER SECURITY POLICIES FOR THE INDONESIAN NAVY (U)

. PERSONAL AUTHOR(S)
ntonius Herusutopo

a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
aster's Thesis	FROM 03/91 TO 06/93	June 1993	137

. SUPPLEMENTARY NOTATION The views expressed in this thesis are those of the author and do not reflect the fficial policy or position of the United States Department of Defense or the Indonesian Government.

COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	SECURITY, COMPUTER, policy, Indonesian Navy

. ABSTRACT (Continue on reverse if necessary and identify by block number)

The Indonesian Navy recognized the need for a computer security program over ten years ago. They published eir first computer security regulation in 1981. But that regulation is now obsolete because of the advances in chnology and increased availability of powerful computer systems. As computer systems become bigger, more mplicated, easier to use, more interconnected, and more important, they become more vulnerable to hackers, rrorist, and disgruntled employees.

This thesis demonstrates the need for an updated computer security regulation. To add in meeting that need, the esis proposes a security program for the Indonesian Navy that is based on the multilevel trusted computer criteria iblished by the NCSC in the 'Orange Book', the Canadian Trusted Product Evaluation Criteria and ITSEC. The oposed program includes additional regulations concerning physical security, data security, integrity and ailability, and recommended trusted evaluation guide.

. DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
a. NAME OF RESPONSIBLE INDIVIDUAL imothy J. Shimeall	22b. TELEPHONE (Include Area Code) (408) 656-2509 — 22c. OFFICE SYMBOL CSSm

FORM 1473, 84 MAR — 83 APR edition may be used until exhausted. All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

Approved for public release; distribution is unlimited

A STUDY OF COMPUTER SECURITY POLICIES FOR THE INDONESIAN NAVY

by

Antonius Herusutopo
Major, Indonesian Navy
B.E. Electronics Engineering, Naval Electronics School, 1972

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
June, 1993

ABSTRACT

The Indonesian Navy recognized the need for a computer security program over ten years ago. They published their first computer security regulation in 1981. But that regulation is now obsolete because of the advances in technology and the increased availability of powerful computer systems. As computer systems become bigger, more complicated, easier to use, more interconnected, and more important, they become more vulnerable to hackers, terrorist, and disgruntled employees.

This thesis demonstrates the need for an updated computer security regulation. To add in meeting that need, the thesis proposes a security program for the Indonesian Navy that is based on the multilevel trusted computer criteria published by the NCSC in the 'Orange Book', the Canadian Trusted Product Evaluation Criteria and ITSEC. The proposed program includes additional regulations concerning physical security, data security, integrity and availability, and recommended trusted evaluation guide.

H52125
c.1

TABLE OF CONTENTS

DUDLEY KNOX LIBRARY
NAVAL POSTGRADUATE SCHOOL
MONTEREY CA 93943-5101

LIST OF FIGURES

ACKNOWLEDGMENT

Grateful acknowledgment must be made to several individuals who have given me help, ideas and encouragement during the process of writing this thesis. I would like to acknowledge the late Professor Uno R. Kodres, who encouraged me to start writing a thesis and my thesis advisor Professor Timothy J. Shimeall and Roger Stemp who gave their knowledge and support throughout this process. I would like to thank my thesis editor Phil Anderson who greatly assisted me to in the actual writing of the thesis. Thanks also to Rear-Admiral Sutanto and Commodore L. Handoko who encouraged and supported in my thesis efforts. Finally, special thanks to my wife and my children Wiwiek, Bona, Aji and Bayu Herusutopo, for their support and patience during the past two years at the Naval Postgraduate School.

I. INTRODUCTION

A. COMPUTER SECURITY IN GENERAL

As computer systems have developed, they have produced spectacular changes in many organizations, affecting everything from office correspondence and personnel data processing to real-time process control. With computer systems, great amounts of paper records are no longer needed, reducing storage requirements and the time needed to search records. Computer systems have brought many improvements.

This valuable tool requires protection. That protection is what computer security is all about. Computer security means protecting the computer and everything that is associated with it. These associative items include the room or building, the terminals and printers, the cabling, and the storage devices such as disks and tapes. Most importantly, computer security means protecting the information in the system [RUSS91, p. 8].

For many years computers were isolated from the outside world. Security required only securing the room or the building and controlling the people that programmed or operated the computers. Links to the outside were unusual. Computer security threats were rare, and were basically concerned with insiders: authorized users misusing accounts, theft and vandalism [HOLB91, p. 6]. A good lock and a security guard were enough to secure the computer from any physical attack.

With the development of communication networks, computers were connected to one another: first by specially-engineered dedicated lines and then by common telephone lines. Now many systems are in private offices and labs, often managed by individuals employed outside a computer center. Many of these systems are connected to the Internet where they have access to and can be accessed by systems around the world. The United

States, Europe, Asia, and Australia are all connected [HOLB91, p. 6]. Many of these computer systems, such as the systems used in banking, operate 24 hours a day. Thus, the definition of computer security has grown well past the locked room with a guard at the door.

While the fundamental concepts of computer security, protect the information and the equipment, are the same, applying these principles is much more complicated. Computer security consists of maintaining three characteristics: secrecy, integrity, and availability [PFLE89, p. 4]. Secrecy, also called confidentiality, means that only authorized persons can access the information assets. Integrity means that only authorized persons can modify the information. Availability means that the information is always available for authorized use.

The effectiveness of a security program is highly dependent on the attitudes and amount of security training that the personnel using the system have. To maintain its value, the security program must continually be reviewed for effectiveness and relevance. In every organization, security should be made an integral component of the corporate culture and made a personal issue for all. In many quarters there is still a lack of security awareness among corporate and organization managers. Quite often, any awareness that does exist is limited to the more obvious physical requirements. [DITT90, p. 30]

To create a secure operating environment the computer system must be viewed in terms of what can damage it or compromise the information it contains. That is, it must be reviewed in terms of its vulnerabilities. Any occurrence that can damage the system at one of these vulnerable points is a threat. Computer security is concerned with identifying the threats to the system and protecting against those threats. [RUSS91, p. 11]

Russel and Ganggemi [RUSS91, p. 12] divide threats into three (3) categories: natural, unintentional, and intentional. A typhoon or an earthquake may not intend to do damage, but can destroy the system. The curious employee that walks over to a new

terminal and spills a cup of coffee into the monitor probably did not intended to destroy any equipment, but the system must be secured against him as well as the digruntled employee that did not get promoted and tries to erase all the financial reports for the last three years. A comprehensive computer security program must recognize and plan for all these disasters and many more.

B. COMPUTER SYSTEMS IN INDONESIA

The computer industry is very young in Indonesia. In general, computers are a great luxury. Very few persons or industries have access to computers. Common society views computers as "very clever things." They don't believe they can use these clever things. Managers view computers as devices made by men and therefore very unreliable. Schools and universities do not offer computer science as a separate course of study. Rather, courses are offered as part of another curriculum such as electrical engineering. Furthermore, there is almost no industrial base; the majority of all hardware and software is imported from Japan and the United States, with some components imported from Korea, China and Singapore.

The threats to the computer and information systems can be very sophisticated. As in many countries, there are always individuals that are much more capable than the general public. If a terrorist group wanted to hurt the government and they could not recruit a local person with the necessary expertise, they could hire someone from another country. Because most people are unsophisticated, it is easy for the system operators and users to become careless about enforcing the security program. This provides just the opening that a hacker needs. Additionally, due to the lack of copyright laws and the relatively high price of new software, there is a tremendous amount of passing copies from user to user, providing optimum conditions for spreading viruses and worms. The computer security regulations must deal with both of these threats.

Currently, there are several mainframe computers that are being used by industry and government. The banking industry was the first industry to utilize an information system, primarily to automate their accounting systems; however it is still unusual to see a teller with a front-end terminal. There are two (2) primary reasons for this; first, acquisition and installation are still relatively expensive. Second, and perhaps harder to overcome, managers do not trust the tellers to send information directly to the computer. Network connections between the main office and the branch offices have not been installed yet, mainly because security problems have not been resolved.

The biggest government user of automation is the Department of Defense (DoD). The DoD currently uses computers mainly in support of personnel, payroll, and logistics management. As real-time computing has advanced, the DoD is increasingly developing and acquiring computers for combat systems. As a result of this growing reliance upon real-time information systems the Department of Defense built a computer center to support the software used in combat systems.

Several other Government offices use computers to support their efforts. Computers are used for producing documents such as ID cards and drivers licences. But use is limited to the larger cities because of the lack of spare parts and maintenance personnel in the rural areas.

The telecommunications network is still too immature to support modem connections. The backbone systems are terrestrial and satellite microwave with some larger cities using sea cables. The phone system itself is not computerized, it relies almost exclusively on human operators. Cross talk and interference are routine problems because of physical plant limitations. And there is insufficient channel capacity for the voice traffic alone. The use of more satellite capacity is the best chance for increased modem activity.

As indicated above, there is no commercial software development in Indonesia. Both operating system software and application software originates in the United States or

Japan. One barrier to local software production is the lack of effective copyright protection. Software piracy is a regular occurrence because of the weak laws. These laws will have to be strengthened before there is an incentive to write computer programs.

C. THESIS OBJECTIVES

Since the current standards and regulations in use by the Indonesian Navy were written in 1981, and today the Navy is installing a series of computers operating over a local area network (LAN), which is expected to grow until it is interconnected nationwide, than the objectives in writing this thesis are:

1. To conduct a literature search of computer security articles.

2. Review and critique of the current computer security policies of the Indonesian Navy.

3. To develop a strategic computer security policy for the Indonesian Navy.

D. THESIS ORGANIZATION

This thesis is presented in five (5) chapters. Chapter II provides the fundamental concepts of computer security, what standard regulations are needed, and provides a preliminary threat assessment and the controls needed to protect it. It also explains some models for Multilevel Security and some security issues from the United States, United Kingdom, Germany and Canada.

Chapter III is a review of the current computer security policy of the Indonesian Navy, the computer systems being used and the policy elements that need to be upgraded. Chapter IV outlines the need for a computer security policy for the Indonesian Navy and proposes an evaluation guide for the Indonesian Navy as a basic step for implementing multilevel security in computer systems. Chapter V includes a summary, conclusion and

recommendations. These recommendations define immediate, intermediate and long term actions should be taken concerning computer security.

The appendix contains the recommended Trusted Evaluation Guide for use by the Indonesian Navy.

II. FOUNDATIONAL CONCEPTS OF COMPUTER SECURITY

There are several concepts that serve as a foundation for a good computer security program: maintaining system integrity, protecting privacy, and building a cost-effective security program. The best method for satisfying these criteria is a trusted multilevel security system.

To achieve the goals of computer security, that is maintaining the three characteristics of privacy, integrity and cost-effectiveness, the first thing to do is recognize the threats to the computer system. By recognizing the potential threat, the actions to defend against those threats can be defined.

A. COMPUTER SYSTEM INTEGRITY

The first step is to physically isolate and protect the system. The goal is to keep hostile forces out of the system. Second, if the hostile force gets into the system, then the system must be able to identify, contain and record the actions of the infiltrator. Finally, it is important to establish sound backup procedures to facilitate recovery in event of complete contamination or destruction of the computer system.

Maintaining computer system integrity begins with securing the system against the most basic threats: storms, floods, power failures, and progresses up to the most sophisticated threats: espionage agents planted in user organizations, electronic eavesdropping, and computer hackers with their own advanced computers. The organization cannot install a security system and forget about it; the system must be constantly reviewed to keep pace with the evolving threat and re-evaluated against the growing dependency of the user organizations on the automated systems.

1. Physical Integrity

Physical protection is the most important measure of computer system security. If the physical security of the system is not guaranteed, then the system can not be considered secure. This physical protection includes the guard, the room and building construction, the door lock, fences around the building, etc. These protect the system from natural disaster, human vandals, interception, and unauthorized user.[LANE85, p.13 -18, PFLE89, p.437 - 442, and RUSS91, p.238 - 240]

Natural disasters like floods, fires, earthquakes, lightning, power loss, heat, etc., constitute a threat to the physical integrity of a computer system. Not only is the physical hardware at risk, but also the information residing in the system. In many, cases the information is more valuable then the hardware itself. [PFLE89, p. 438]

One natural threat is water, which can easily damage the electronic components and electrical systems used to support it. Water damage can occur because of the flooding of a river or the sea, a hard rain or even a leaking water pipe. To prevent this kind of disaster the computer system should be placed in a room high enough to be unreachable by water that rises from the ground.

In addition to flooding, water falling from above the equipment is also dangerous. This is usually caused by a leaking water pipe above the equipment or a leaking roof or ceiling. In order to prevent this kind of disaster the administrator should regularly inspect the possible sources of water damage. Secondly, rolls of plastic sheeting should be mounted on the walls of the computer room so that the equipment can be covered in a matter of minutes in case of an emergency.

Fire is another natural disaster that can cause great damage quickly. In order to prevent this kind of damage water is not recommended, since water also damages the electronic devices. A fire resistant wall and door, and a windowless room for the computer

installation is suggested in order to slow the spread of fire from adjacent rooms. Furthermore, smoke detectors and automatic fire extinguishers using inert gases are recommended for fire suppression.

Electrical power systems are critical to computer systems. If the power is suddenly lost or drops below a certain value, the possibility of losing code or data that is not yet saved becomes almost certain. To prevent loss of code or data caused by a power loss an uninterruptible power supply is recommended. An uninterruptible power supply stores electrical energy during normal operation and is automatically turned on when the power is lost.

Protection against spikes or surges of electrical power is also required. If a spike exceeds the specified level of the equipment, then it can damage the electronic components. In order to prevent this, a surge suppressor is needed.

Heat is another natural problem common to tropical countries like Indonesia. Electronic components inside the computer system are sensitive to heat. If the heat exceeds a certain level then the components may work improperly or sustain damage. Preventing the accumulation of excessive heat requires a continuous flow of cold air.

Humans also pose a threat to the physical integrity of the systems. Vandals and disgruntled employees may intentionally damage the system, and users and visitors may unintentionally cause damage. All of these are threats to the physical integrity of the computer system.

Defending against vandals is an important feature of physical protection. Vandals are different from natural disasters, since the damage is intentionally or unintentionally caused by people. They can be disgruntled employees, bored operators, saboteurs, or people that get a thrill from destroying things. If their tool of destruction is something that is big enough to see, such as a sledge hammer, then they can be stopped before they damage the equipment. If they use small items, such a car key or even a paper

clip to disable a disk drive, then it will difficult to detect them before they strike. A strict visitor control policy will help reduce this threat.

Physical damage remains the greatest threat to computer security. The next section explains threats against software and data integrity.

2. Software And Data Integrity

Attacks on the software and data are more difficult to prevent and track, since the damage may not be visible, but they can completely disrupt the operation of the system. Deletion or modification of valuable data can cause grave damage to individuals, organizations or even whole nations. The damage caused by or actions done by human threats may go completely unnoticed by the operators until the results from the system differ from what is required on a given situation.

The threat to software can also come from an unintended source. Some programs produce unintended results, degrade system efficiency, or destroy data. While this is not deliberate sabotage, the effects are significant and must be mitigated. In an ideal world, damage to a system by unintended results would be prevented, but research and practice in the area of system reliability has shown that this ideal protection is unlikely in the foreseeable future.

a. Internal Threat

The most difficult threat to counter comes from inside the organization itself. A malicious worker can introduce a virus or do many kinds of damage to the system, which may be done in a such manner that it remains undiscovered for a long time. Furthermore, an innocent employee may damage the system without realizing it. A hard-working employee may bring work home, infect his disk and bring it back to work and infect the system. Good backups, archiving and antivirus software will mitigate most of

the damage caused by infection. A system of file protections, not modifiable by ordinary software, will prevent the spread of many viruses.

Depending on the security of the computer system, it may be possible for an employee to change the classification of a file. An employee with a high-level security clearance, who can access a highly-classified file, may intentionally or unintentionally change the classification of a file to a lower level, or disclose it to an unauthorized employee or an external agent: any of which could cause great damage.

Modification of the software must also be controlled. Without such controls, changing a little code in a program can be done by anyone. The program may seem to work well, but in a specialized condition the program will fail [PFLE89, p. 7]. One example of this type of modification is a time bomb. An infected program will work well in almost all cases, but upon detecting a specific condition, such as a system load level or the name of a certain operation, the program will fail or do some other damage to the system.

Programs need to be secured since they can be used to exploit vulnerabilities in computing system in one of two ways. First, they can intercept or modify data on behalf of users not authorized to access the data. Second, they can exploit service flaws in system to allow system access to unauthorized users and inhibit the use of legitimate users. Some programs commonly used to access data and affect computer services are described below.

(1) Trapdoors. A trapdoor is a secret undocumented entry point into a module. It is usually inserted during program development for testing, maintenance, and debugging purposes. Sometimes it is not removed, and as a result it exposes the system to modification during execution. [PFLE89, p. 170, and RUSS91, p. 85]

(2) Viruses. Viruses are programs that can infect other programs by modifying them. [PFLE89, p. 178] All viruses require a host, and the range and rate of the

spread of the infection depends on sharing and transitivity of programs or data.Viruses must have access to other programs and data in order to spread. Thus, limiting sharing can limit viral infections.

Viruses are prevalent in personal computers because so much software swapped between users that it is easy for viruses to spread to different systems. The weak copyright laws in Indonesia is one reason that there is so much swapping there. The positive side is that software is being developed to combat viruses and can be imported from developed countries. The use of anti-viral software should be stipulated in the security regulation.

A virus program has three parts. The first is a marker that is used to determine if a program has been previously infected (signature byte). The second is the infector which seeks out potential carriers and is responsible for the infection process. The third part is an optional trigger that, upon determining that current conditions match an activation segment, trigger the manipulator. The fourth part is the manipulator that is responsible for carrying out the program's designed task.

Viruses are categorized as either overwriting or non-overwriting. Overwriting viruses are the easiest to write and do not increase the length of the host program. They actually overwrite the code of the host programs and as a result, the host program will generally produce an error during execution.

A non-overwriting virus appends itself to the host program and causes an increase in the file size, actually it copies a portion of the host's code and appends it to the end of the file then overwrites the other portion. During execution the virus checks the trigger and if applicable, executes the manipulation code. Once completed it then moves the host's copied portion of code to the front of the file and executes the host code normally.

Viruses have some known weaknesses. All viruses have markers and the host program has to be executed in order to execute the viruses' codes. They must change some segment, therefore they leave tracks of their presence.

There are many types of viruses: boot sector viruses, system software viruses, application software viruses, hardware viruses placed by actually modifying the hardware, buffered viruses that install themselves in RAM, live and die viruses that remain for a certain period then remove themselves, and hide and seek viruses that move to different areas of the system.

A few of the ways to limit the spread of viruses are: complete isolation of infected systems, subdivision of data and programs, write protect all disks that are not to be written to, don't share disks, on the fly encryption, and limiting transitive flow of information (A to B, B to C, thus A to C).

(3) Trojan Horses. A Trojan horse is a program that performs a hidden function in addition to its stated functions. A virus can carry a Trojan horse program, such that the infected programs perform an unintended function. [PFLE89, p. 172, and RUSS91, p. 83]

(4) Covert channels. A covert channel is a program that leaks information to people who should not have it; they are a hidden means to communicate information. They are best suited to situations where small amounts of data are needed.[PFLE89, p. 175]

(5) Worms. A worm is a program that can run independently and can propagate a fully working version of itself on other machines. Worms do not need a host, they are self propagating and stand-alone. Not all worms are malicious, as a matter of fact, some worms are beneficial they perform automatic file compression and backup. [PFLE89, p. 178, and RUSS91, p. 82]

b. External Threat

Any outsider who has a connection with computer system may succeed in infiltrating the organization and gaining access to the computer system. Then he can read, modify, delete or copy the software or data. This is an external threat that should be considered.

As the Indonesian Navy starts to develop Local Area Networks (LAN) and computer systems become inter-connected, it will be easier to conduct attacks on one system from several remote hosts or many systems from one host. The modification of data in a system is very difficult to recognize and to track since the host may not know that some of its information has been modified by an unauthorized person.

An external intruder typically attempts to access a computer system through the telecommunications networks. Several different types of attack may be attempted and once access to the system has been achieved, the intruder may cause significant harm to the system or the data.

Threats to hardware, software or data may cause severe damage to a computer system. The next section explains what steps can be taken to minimize the damage if all the planning fails to prevent damage.

3. Resumption after a Crisis

Security planners must assume that eventually they will fail and the system will suffer severe damage. A recovery plan is needed in order to get the computer system working as soon as possible. It can be achieved effectively if there is enough preparation. It has been mentioned above that damage to the computer system can happen to the hardware, software or data. To prepare for damage to the information, backup copies are needed. If the damage is to the equipment, then a backup facility is needed.[PFLE89, p. 442 - 447, and RUSS91, p.96]

A backup is a copy of all the software and data residing in the computer system. A periodic backup needs to be performed so that the loss is limited to the work done during the interval between backups. However, if the backup copy is maintained in the same place, or near the same place, that the computer system is located then it can be rendered useless, because the backup copy can also be destroyed during the crisis. Thus, backups should be stored off-site.

Just as the data and programs are backed up, the hardware can be backed up. Either a cold or a hot site can be used, based on the criticality of the system. A cold site is used when the system is relatively less critical and time to outfit the facility is available. A cold site has space, power and air conditioning. If the primary site is destroyed or severely damaged, then new equipment is installed and the operation is moved to the backup site.

A hot site is used when the applications are critical. A hot site is a computer facility with an installed and ready-to-run computing system [PFLE89, p. 444]. A hot site not only has the space, power and air-conditioning, but also a complete computer system. All that is required to get operational is load the latest backups and begin processing. Obviously, to prepare and maintain a hot site is very expensive and can only be justified when losing the processing system for several days or weeks would be more expensive. Hot sites are reserved for systems processing critical data and applications.

B. PRIVACY

There are certain differences between privacy and security. Privacy is a characterization of the special interest we have in being free from certain kinds of intrusion [JOHN85, p. 194]. Privacy is strongly rooted in ethics and morals. James Martin's definitions show the important distinction between privacy and security. Data security refers to protection of data against accidental or intentional disclosure, unauthorized modifications, and destruction. Privacy refers to the rights of individuals and

organizations to determine for themselves when, how, and to what extent information about them is to be transmitted to others [MART73, p. 5].

The value of informational privacy depends on the situation and the ownership condition of the information itself. An individuals bank balance is important to the individual, but compromising it is not likely to damage national security. If an important company is taken over by foreign competitors because private financial information was compromised, then national security may very well be damaged. Additionally, the perceived value of privacy varies from culture to culture. Societies establish and enforce privacy laws very differently, with liberal societies providing the greatest protections and totalitarian societies the weakest. Whatever the society, there is some cultural or legal protection of privacy.

With improvements in computing systems, most private individual data is being entered into computer records. For example in the military, some information may only be read by the commanding officer, other information may be read by all officers, and some information by all officers and enlisted. However, all this information may be kept in computer records. As a consequence, privacy may be lost if the security system is inadequate. Absolute privacy requires absolute security. There are no systems that provide absolute security, but a trusted system will provide the best possible protection available.

It is obvious that the technology of privacy is closely related to security, however, privacy is an issue that goes far beyond the computer system. Furthermore, implementation of security to protect individual privacy in a computer system should be calculated according to its cost effectiveness despite the inherent difficulties in establishing the value of an individual's privacy to the organization installing the security system.

James Martin defines four (4) levels of safeguards needed to protect the privacy of individuals [MART73, p. 32 -33]. The first is locking the data in the system so that

unauthorized user cannot read, modify, delete, or copy it. The second is an appropriate system philosophy that specifies how the computer system should act on the individual data, how the system will control which person can access each kind of data, what data should not be collected and what classification should be assigned to the data. The third level defines administrative controls and the fourth defines legal controls. The legal controls are defined by existing law concerning the protection of privacy in the computer system. The law concerning privacy depends on the culture and national philosophy. In the liberal society the individual privacy is stated clearly, but in some other countries, the laws protecting privacy, especially those concerned with computer technology do not exist yet.

1. Theft Prevention

Unauthorized visitors can cause three problems: stealing machines or data, destroying machines or data, or compromising the data, which can be very dangerous if the data is very sensitive [PFLE89, p.444]. Some precautions can be taken to protect against theft such as security guards, fences, locks, magnetic stripe cards, electronic cards, and even gluing, weighting, chaining, and alarming portable devices.

Security guards, fences and locks are classical examples of theft prevention. Guards have an advantage in that they can make a record of persons who access the facility. However, guards must be employed 24 hours a day. And as human beings they have human weaknesses that can be exploited, such as boredom, inaccuracies, illness, etc. As a result, their reports may be inaccurate and they may even be so careless that they fail to catch a thief. On the other hand, locks are much simpler and cheaper to use, but they may not produce the record that is desired. The best system is a combination of guards, fences and locks.

More sophisticated controls use magnetic stripe cards or cards with radio transmitters or other electronic identification system. These systems can interface with a computer system which can automatically prepare an access report. The disadvantage is that they can be lost or stolen and the finder can have access to the facility. To prevent unauthorized persons from getting into the facility, the cards can be supplemented by a keypad at the door that requires some kind of entry code from the person trying to get in.

Reducing portability of the equipment will also reduce the risk of theft. Portability has increased as more powerful and expensive devices are built to fit on a desk top. Some facilities use these kinds of computers for interfacing with a mainframe. Even input/output devices, such as printers, are now portable devices. Since it is portable, it is easy to steal. Steps must be taken to reduce theft, but excessive measures can make the system difficult to use by the very persons it was installed to support. Measures commonly used to protect the equipment include adding weights, gluing the equipment to a table, chaining or locking the equipment down, or installing alarms. The weights and glue make it difficult to move the equipment if there is a problem. Chains, locks and alarms are better in these situations because they can be undone relatively quickly.

In addition to securing the equipment, attention must be given to taking care of sensitive files. Printing a sensitive file should only be done when unauthorized personnel are away from the printers. One option is to configure the system so that classified files can only print on a printer in a secured area.

The last method for controlling theft is to install detectors in the door. These detectors can sense individuals coming into or leaving the facility. If used in combination with smart cards the detectors can even record which person comes and goes. This can help reduce unauthorized traffic. But to prevent authorized users from taking equipment, the equipment can have internal marking devices that will set off the alarms if they are carried through the exit.

Ideally, software theft will also be countered. Specifically, the security system will prevent unauthorized copying of software. Since the original software itself is left unchanged in the system, the owner has no indication that a theft has occurred.

Interception is another serious threat to computer security. To illustrate: a repairman from outside the organization is responsible for repairing any damage or malfunctions in the computer equipment. He can install a device that will be able to read data and transmit it to a receiver that is outside of the secured area. Hence, valuable or critical data is compromised. To avoid this, the technicians should submit to the same clearance procedures that the operators submit to.

2. Disposal of Sensitive Media

Disposal of sensitive media may create a vulnerability. Media containing sensitive information often needs to be disposed of. The media can be paper, magnetic tape or disks, printer ribbons, or even paper tape. They may have to be disposed of because they are no longer useful, such as outdated reports, or the magnetic media may be damaged. But even damaged media can be reconstructed if it falls into unfriendly hands. The media must be destroyed beyond any ability to extract useful information. There are many ways to dispose of these material. [PFLE89, p.446]

Shredders are the most common devices to use. They can be used to destroy paper, printer ribbons, floppy disks and some tapes. The disadvantage is that the most common shredders cut the media into long strips that, in the case of paper, can be reconstructed and read. In these cases shredding is only an intermediate step to burning. The reason to shred the paper before burning it is that the burning is then much more thorough.

There are several ways to destroy the information on magnetic media. The most common is to overwrite the data several times with different characters. But this takes a

certain program or utility. For many years users thought they were destroying their files by deleting them, but most operating systems only released the disk space back to the system. The data could remain on the disk and some other person could recover it with another utility. To prevent this a write-three-times utility must be used when clearing files or media. This can be a very time consuming requirement, but it is necessary to protect the data.

Another way to erase the data is to use a magnetic degausser. A degausser is a powerful magnet that realigns the magnetic particle and destroying the patterns that stored the data. Some degaussers are moved over the media, others are built so that the media passes through the magnets. This can be an effective method, but the degaussers must be tested periodically to ensure that the field strength meets the specifications.

3. Emanation Protection

Emanation protection is divided into two categories. They are: protection from outside emanations that can affect the operation of a system, and control of emanations from the computer devices that can be detected outside the controlled area [PFLE89, p. 447- 441].

First, emanations that affect operations can originate inside or outside the facility. Many components of a computer system are sensitive to magnetic fluctuations. For example, a floppy disk is sensitive to the magnetic fields produced by the electromagnets in devices such as telephones, printers, and monitors. The data on the disk can be ruined by these fields if the disk is set on or too close to this type of device. The administrator should stress the vulnerabilities of magnetic media to the workers.

Secondly, the emanations from the equipment can be intercepted by persons outside the are controlled by the users of the system. In some cases these emanations can be demodulated and the data that the machine was processing at the time is compromised.

A standard acceptable level of emanations and proper control procedures should be determined and included in the security regulation. Some methods of control are: using low emanation devices (TEMPEST approved), shielding the room or using shielded containers around the worst equipment, and expanding the controlled area to a point that the emanations are no longer detectable.

4. User Authentication

Computers need to verify users with authentication mechanisms, usually at the time they log on. Authentication mechanisms are generally divided into three categories: something you know, like a password; something you have, like smart card; and some unique attribute, such as a finger print. [RUSS91, p. 57 -58]

The most common authentications used on computer systems are passwords. They are easy to implement and a person only needs to remember his password to access the system. The password is a string of characters, a "word" that the computer is programed to ask for when the user logs onto the system [PHLE89, p. 226]. The effectiveness of is limited by their length and the number of legal characters allowed in each position. Because they are limited in length and because they must be remembered by people with many things to remember, they are vulnerable to attack.

Basically, there are five different attacks that can be used to break a password system. They are: try all possible passwords, try many probable words, try words likely to be used by an individual user, try to find the system password file, and to ask the user.

Trying all the possible passwords is called the exhaustive attack or brute force method. If given unlimited time and attempts, the user will find the right word. This method can be frustrated by using words in excess of seven characters and using all the letters (upper and lower case), numbers and characters on the keyboard.

The probable password approach attempts to use common words that users are likely to use. Because passwords are to be remembered, most people will attempt to make one that makes sense. A random string of characters is difficult to remember, so the user will choose a word or a group of letters that is almost a word. This narrows the universe that the intruder needs to try and greatly increases his chance of penetration.

The next method is to identify a particular user and learn as much about him or her as is possible. Then the intruder can build a list that the user is likely to pick a password from, such as the name of a child, a pet, a favorite car or fiction character, or anything else that the user favors. The smaller the list of words that the attacker needs to try, the greater his chance of success.

Finding the system password file is a different kind of approach. If the attacker can get any level of access to the system, he can try to find the list of passwords. This will allow him to access anything on the system. Because the list is so powerful, the systems administrator must take steps to protect it, such as locking the file so that only the administrator can access it and encrypting the file so that it can not be read by the intruder if it is discovered.

Getting the password from a user is the easiest way of penetrating the system. Sometimes a group that works together will share their passwords to simplify the work. This will make the work simpler, but it will also weakens security.

There are several choices that the security administrator and users can do to enhance the security value of the passwords. This selection is provided by Pfleeger. [PFLE89, p. 232 - 233, and RUSS91, p. 61]

(1) Use more than A-Z

(2) Choose long Passwords

(3) Avoid actual names or words

(4) Choose unlikely passwords

(5) Change passwords regularly

(6) Don't write them down

(7) Don't tell anyone else

The suggestion above should be stated clearly in the regulation concerning password selection criteria.

A more sophisticated authentication system uses identifications and passwords followed by a challenge and response interchange. The system asks different questions each time, and must be replied to with correct answers; therefore, it is also called one-time password. This authentication system is secure since interpretation of passwords is very difficult. However, it is limited by the capability of people to remember the responses.

Another kind of password system uses a passphrase, which is a longer version of a password. A passphrase consists of a number of words to form an easy to remember phrase. Passphrase are easier for users to remember and since the are longer than passwords they are inherently more secure. A limitation of passphrases is that they require more memory to store.

Smart cards or tokens can eliminate need for people to remember passwords. One example is the magnetic stripe cards used by banks for automatic teller machine service. The disadvantage of tokens or smart cards is that they are easy to lose.

A perfect authentication system that can never be lost and has nothing to remember uses a personal characteristic such as a fingerprint, retina pattern, or the user's voice pattern. They give high a high level of assurance and reliability since each personal characteristic for each person is unique. The disadvantage is that these systems are very expensive. [PFLE89, p. 391 -392]

5. Encryption and Decryption

Encryption and decryption are computer security methods used to make it difficult for intruders to read any data even if they do break into the system. Encryption is a process of encoding data and programs so that they are meaningless without the algorithm and the key. The clear message is called plaintext, and the encrypted form is called ciphertext. The reverse process of transforming ciphertext back into plaintext is called decryption. [PFLE89, p.23] To ensure protection, it is important to study the ciphertext regularly to ensure that it can not be easily decoded without the key.

There are many encryption and decryption methods, such as substitution and permutation (transposition). In the development of codes, cryptographers work on encryption algorithms which are hard to break; that is, they develop encryptions such that breaking the encryption is equivalent to finding an object in a search space that has been proven to require more than polynomial time to search (i.e., the search is NP-complete). Presently, three encryption methods are known that are hard to break, although they are not proved yet to fit in this category: the Merkle-Hellman knapsack encryption, the Rivest-Shamir-Adelman (RSA) encryption, and the Data Encryption Standard (DES).

The Merkle-Hellman encryption was shown to have serious design weaknesses, so we only discuss the Rivest-Shamir-Adelman (RSA) encryption, which has remained secure until this time and is used in some European countries, and the Data Encryption Standard (DES) that is broadly used in the United States.

a. Rivest-Shamir-Adelman (RSA) Encryption

The RSA encryption algorithm was introduced in 1978, and remains secure to this time. The RSA algorithm uses a solution of number theory complicated by the difficulty of determining the prime factors of a target.

Basically, the RSA algorithm operates with arithmetic mod n. Two keys, d and e, are used for decryption and encryption. A key is a certain value of integer that used to encrypt or decrypt a text, these keys only known by the sender and receiver of the messages. The plaintext P and the ciphertext C are treated as positive integers. A plaintext P is encrypted into a ciphertext C by

$$C = P^e \bmod n$$

And to decrypt the ciphertext, use

$$P = C^d \bmod n$$

The encryption key e and decryption key d are chosen such that

$$P = (P^e)^d mod\ n$$

Due to the symmetry property of modular arithmetic, these encryption and decryption formulas are mutually inverse and commutative, hence:

$$P = C^d mod\ n = (P^e)^d mod\ n = (P^d)^e mod\ n$$

The encryption key consists of a pair of integers e and n, and the decryption keys are d and n. To ensure that an intruder will take a very long time to break the ciphertext, these integers should be large. First, choose n as a product of two primes p and q which are two large prime numbers. Next, a relatively large integer e is chosen relatively prime to (p - 1) * (q - 1). Finally, select d such that

$$e \times d = 1 \bmod (p-1) \times (q-1)$$

Choosing numbers which are large and prime increases the difficulty to break the RSA algorithm. [PFLE89, p.101]

b. *Data Encryption Standard (DES)*

The Data Encryption Standard (DES) was developed by U.S. Government for use by the general public. It has been accepted as a cryptographic standard by the U.S and other countries. [PFLE89, p.106 - 121]

By design, DES is composed of substitution and permutations (transposition). The exploitation of these two techniques are repeated for 16 cycles, each cycle stacked on top of the others. The plaintext is encrypted in blocks of 64 bits, the key used it is also 64 bits long although only 56 bits are needed, and it can be changed as needed. The substitutions provide confusion by systematically substituting one bit pattern for another; the permutations provide confusion by reordering the bits. The DES algorithm uses only standard arithmetic and logical operations with results limited to 64 bits. Therefore, it can be implemented in current software and also on a single-purpose integrated circuits. In fact, several DES chips are already commercially available.

The DES algorithm starts by dividing the plaintext input into blocks of 64 bits, and then transforming them using 64 bit keys. The 64 bit input data blocks are pre-permuted by the initial permutation, and broken into 32 bit right and left halves. Then the following process is applied 16 times.

(1) The right half side is expanded from 32 to 48 bits by expansion permutation; it permutes the order of the bits and repeats certain bits. This expansion has two (2) purposes: first, to make the intermediate halves of the ciphertext comparable in size to the key; second, to provide a longer result that can be compressed later on.

(2) The 64 bit key is cut into a 56 bit key by deletion of every 8th parity bit; then split into 28 bits right and left side, each of them are shifted left by a number of bits then pasted back again. After being shifted and pasted back again, the key is reduced from 56 to 48 bits by permuted choice.

(3) The 48 bit key is combined with the 48 bit expanded right half side of ciphertext done in sub (1).

(4) The 48 bit result is divided into eight six bit blocks; each block (B_i) is operated by an S-box (S_i), which performs substitution replacing 6 bits of data with 4 bits.

(5) The 32 bit result (eight four bit blocks) is then permuted by a straight permutation P-box.

(6) The 32 bit permuted result is combined in X-OR functions with the 32 bit left side to perform a new right half for the next cycle.

(7) The old right half side becomes the new left half side for the new cycle.

Then the cycle is repeated fifteen times. At the end of sixteenth cycle, the right and left half sides are pasted together, and by applying inverse initial permutation to get the output. The same algorithm is used to decrypt the ciphertext, only the key applied to decrypt is used in reverse order of the encryption key.

The only known weaknesses in this algorithm are weak keys and semi-weak keys. Weak keys occur if the bits of the key are all zeroes or all ones, it does not change in permutation and substitution; the semi-weak keys are keys with obvious patterns. For other keys this algorithm is secure.

C. COST EFFECTIVENESS

One of the most important measures for evaluating a computer security policy is to ensure that expenditures on security yield cost-effective benefits. Although this may seem obvious, it is possible to be misled about where the primary effort is needed. [HOLB91, p. 10] One method used to determine cost-effective measures is risk analysis. Risk analysis estimates how much it will cost to prevent damage or to recover from specified damage or loss.

Pfleeger defines six (6) basic steps required for a thorough risk analysis. [PFLE89, p. 458] They are: identify assets, determine vulnerabilities, estimate likelihood of exploitation, compute expected annual loss, survey applicable controls and their costs, and project annual saving of control. The person performing the assessment identifies the

assets by listing the system components, including: hardware, software, data, people, documentation, supplies, etc. To calculate the replacement cost of software and data may be as straightforward as finding the bill or as complicated as estimating the number of man-hours to reproduce a study or rewrite a program. In addition to the replacement cost the analyst must estimate the cost of disclosure, such as having a ship destroyed because its planned route was compromised. Determining the vulnerabilities means taking into account all the possible threats to the computer system. Some of the possible threats are natural disasters, human vandals, unauthorized access, disclosure of information, denial of service, etc. Of course, authorized persons have a need to access or disclose information. Security controls must allow authorized users to access files they are authorized to use without letting them access files or programs that exceed their authority. In the past this was accomplished through physically separated redundant systems. It is now technologically possible to operate a multilevel security system (MLS) that permits multiple users, with varying clearance levels, and access abilities (also of different levels of sensitivity) to use the same system without compromising security.

The next step is estimating the likelihood of exploitation. There are several ways to do this: using statistical tables, observing the number of occurrences in a given amount of time, or by group consensus. The annual loss expectancy can be calculated based on the value of an asset and the determination of the likelihood of exploitation. Next, a survey of applicable controls to prevent the exploitation of vulnerabilities, and a revised calculation of annual lost expectancy is performed. This yields the cost of securing the system and provides a measure of the cost effectiveness of the recommended controls.

D. MULTILEVEL SECURITY AS A PRIMARY PART OF SECURITY POLICY

Computer security mechanisms are needed to ensure that all information residing on a system is protected from being lost, modified or disclosed by either malicious or careless

users. To provide protection Russell and Gangemi define four(4) primary functions that a computer security system should perform. [RUSS91, p. 56]

First, to ensure that unauthorized users cannot get into the system, a system access control is required. There are several different access control methods that can be applied, like password systems, challenge-response systems, passphrases (longer version of passwords), tokens or smart cards, and personal characteristics such fingerprints, retinal patterns and voice recognition systems. Second, data access controls must define "who can access what data and for what purpose." Through this, the system will support the discretionary access controls that define which other people can read or modify the data, system files, records, fields, user permissions and program permissions. It is also possible to use mandatory access controls, in which case the system enforces access to objects based upon clearance levels. This is required for multilevel security. Third, system and security administrators perform the off-line procedures to prevent possibility of breaking the security system; for example, by clearly delineating administrator responsibilities, by training users appropriately, and by monitoring users to make sure that security policies are observed. The last step is taking advantage of basic hardware and software characteristics in system design to perform appropriate protections; for example, segmenting memory to protect between critical and noncritical data.

1. Models for Multilevel Security

Multilevel security has been modeled after the security classification system used in the military. The military system is divided into four (4) ranks (sometimes called classifications): unclassified, confidential, secret and top secret. In the same way, the users' access is also defined by their ranks; for example, in the Indonesian Navy commanding officers can access the top secret information, officers can access the secret information, and enlisted can only access unclassified information.

One security principle mentioned by Pfleeger [PFLE89, p. 246] is the principle of least privilege. The principle says, a subject should have access to the fewest objects needed for subject to work successfully. This can be explained using the military example above; a commanding officer with permission to access a top secret rank information, is still able to read the secret rank, confidential rank, and unclassified rank information. Furthermore, information access is limited by the need-to-know rule: access to sensitive data is allowed only to subjects who needs to know that data to perform their jobs.

To enforce the need-to-know restriction, the system may use the compartment method, partitioning a rank into compartments. Users are only able to access compartments with information relevant to their job. For example, a commanding officer may not access all compartments in the top secret information rank, but only the part relevant to his job.

As a result, it is possible for information to belong to more than one compartment. For instance, a list of the foreign merchant ships that sail through the passage way of Indonesia may be divided into compartments. For example, the Indonesian Navy, serving as the cost guard, must patrol the passage way. The ships on patrol have access to the complete compartment, the entire list, while other ships and activities can only access information on a certain number of ships, or sub-compartments.

A class or classification is combination of rank and compartments. The users are allowed to access classified information if they have certain clearances. These clearances indicate that the users are trusted to access the information up to a certain level of classification. Similar to the information class, the clearance of the user also defined as combination of rank and compartment.

Recall that the user is a subject, S, and he or she wants to access to a piece of information called an object, O. Then S can access O if:

- the clearance level of the subject S at least as high as the information O

• the subject S has a need-to-know clearance about all information in the compartment.

In mathematical formula the above relation can be expressed

$$O \le S \textbf{ if and only if}$$

$$rank_O \le rank_S \textbf{ and}$$

$$compartments_O \subseteq compartments_S$$

The relation $\le$ is used to limit the sensitivity of a subject that can be accessed to an object, and the relation $\subseteq$ indicates that the compartment of the object is the compartment for which the subject has a need-to-know. It is known that sensitivity requirements are hierarchical, and need-to-know requirements are nonhierarchical.

There are many models proposed for multilevel security (MLS). In this thesis only three (3) will be described since they are used by U.S. DoD Trusted Computer System Evaluation Criteria (TCSEC) for references. They are the monitor model, the lattice model, which can be applied to military environment, and the Bell-LaPadulla model.

a. Monitor Model

The monitor model is implemented by using gates between users, or subjects, and objects. If a user wants to access an object, then he or she invokes the monitor (sometimes called a reference monitor). The monitor takes the request for access and consults the access control information. The contents of the access information file determines if access is granted.

There are two major disadvantages to using monitors. First, if the monitor is heavily used, it becomes bottleneck. Second, it controls only direct accesses. However, this model is used as reference in TCSEC. [PFLE89, p. 243 - 244]

b. Lattice Model

A lattice is a mathematical structure of elements under a relational operator. [PFLE89, p. 248] The relation in the military model is defined through its rank, and it is similar to the mathematical relations. In mathematical relations we use transitive and antisymmetric properties which are defined as follows:

transitive property

if $a \leq b$ and $b \leq c$ then $a \leq c$

antisymmetric property

if $a \leq b$ and $b \leq a$ then a = b

Similar to the military example above, the transitive property is also applied to ranking property. Every enlisted is subordinate to a petty officer, and the petty officer is subordinate to an officer, then the officer subordinates the enlisted. Obviously, the antisymmetric property is also applied in the military, since it is impossible that two members of the same rank will subordinate each other.

c. Bell-LaPadulla Model

The Bell-LaPadulla model is an information flow model, which identifies allowable paths of information flow in a secure system. One purpose of maximum exploitation of computing machines is permitting the machines to work concurrently. It is different from the computing devices of past years, where machines that processed sensitive data were separated from machines that processed unclassified data. Now, a machine should be able to operate with two (2) or more sensitivity levels together without leakage from the higher level to the lower level.

The Bell-LaPadulla model gives two properties that are used to handle security of data in the multiple levels. Basically, the models cover a set of subjects S and a

set of objects O. For every subject s in S, and object o in O there is a fixed security class $C(s)$ and $C(o)$. Then the two properties can be defined as follows: [PFLE89, p. 250]

(1) Simple security property

A subject s may have *read* access to an object o only if $C(o) \leq C(s)$

(2) Star property

A subject s who has *read* access to an object o may have *write* access to an object p only if $C(o) \leq C(p)$.

The simple security property is just like the military security model, and the star property is used to prevent transferring a high level data by an authorized subject into a lower level sensitivity.

2. Database Security

The majority of applications used by the Indonesian Navy involve databases rather than dedicated system such as combat systems on warships. This is understandable since using databases yields advantages such as shared access, minimal redundancy, data consistency (since one changed value affects all users at once), data integrity, and controlled access.

However, the safe exploitation of databases requires security measures such as physical database integrity, logical database integrity, element integrity, auditability, access control, user authentication, and availability [PFLE89, p. 304]. Some situations that affect integrity do damage to the entire database. The element integrity refers to their correctness or accuracy. The DBMS maintains the integrity of each item in three ways: field checks, access control, and change log.

Auditability is desirable in order to determine who did what, and prevent incremental access. However, maintaining an audit trail of all accesses is impractical,

since it is slow and takes a large amount of memory. Databases are logically separated by user access privilege. The database administrator determines who gets access to the data at the field, record or element level; and the DBMS enforce this policy, granting or denying access to all specified data. Usually the DBMS runs on top of O/S, which means that there is no trusted path to the O/S, and the DBMS must be suspicious of information supplied by the O/S, including user authentication. As a result, the DBMS must do its own authentication. Availability should be considered as arbitration of two users' request for the same record, and the withholding of some non-protected data to avoid revealing protected data.

Problems in reliability and integrity can occur when modifying data. If a single field of data is being updated, then half of the field may show old data; if multiple fields are being updated, then no single field reflects an obvious error. To avoid these problems, a two phase update technique is the used. In the first phase (the intent phase), the DBMS gathers information and other resources needed to perform the update, but makes no changes to the database. In the second phase (the commit phase), the DBMS writes a commit flag to the database and the DBMS makes a permanent change. If the system fails during second phase, the database may contain incomplete data, but this can be repaired by re-performing all the activities of the second phase.

Sensitive data management is also another problem. Sensitive data is data that should not be made public [PFLE89, p. 314]. One problem securing a database is preventing disclosure. There are five types of disclosure: exact value of data, lower and upper bound of them, negative result of them, existence of them and probable value of them.

One way to obtain sensitive data is using inference; that is deriving sensitive data from nonsensitive data. This attack can be a direct or indirect attack. Indirect attacks consist of sum (infer a value from reported sum), count (combined with the sum to

produce some even more revealing result), median (requires finding selections having one point of intersection, which happens to be exactly in the middle), tracker attack (adds additional record to be retrieved for two difference queries; the two sets cancel each other out, leaving only the statistic desired), and linear system vulnerability (it may be possible to determine a series of queries that returns results relating to several different sets).

There are three basic ways to control the inference problem. The first is to suppress sensitive data values, insuring that they are not provided and rejecting the query without a response. This may mean rejecting a request that is legitimate if answering the request would reveal sensitive data. The second is concealing the exact value by providing an answer that is almost correct. The third way is tracking what the user knows so that each user that accessed a record can be identified if that record is disclosed.

Multilevel databases offer more than two levels of security, and are based upon military security model explained previously. Multilevel databases have three characteristics: first, the security of a single element may differ from the security of other elements of the same record or from records with the same attributes, thus, security is implemented for individual elements. Second, several grades of security may be needed and may represent ranges of allowable knowledge and which may overlap; typically the security grades form a lattice. Third, the security of an aggregate may differ from the security of the individual elements.

3. Network Security

A computing network is a computing environment with more than one independent processor. It is usually connected through the available communications network [PFLE89, p. 365]. Although the communications system in Indonesia is still too immature to support a computing network, the communications system is being upgraded

and a computer network will be installed. To help understand how to implement network security, a network model is described below.

a. International Standards Organization (ISO) Model

The International Standard Organization has developed a computer communication network model called the Open System Interconnection (OSI) model [PFLE89, p. 366]. There are seven layers in the OSI which range from the user applications to the physical media connections.

The lowest layer is the physical layer; where the physical signal transmissions must be compatible at the bit level. This layer is controlled by the hardware. The second layer is the data link layer, which is also controlled by the hardware. This layer controls communications management functions such as transmission recovery, message separation into frames, optional encryption, headers and trailers, and error detection. The third layer is the network layer; it is the responsibility of the network manager. Routing and blocking messages into packets is done in this layer. The fourth layer is the transport layer; it is also the responsibility of the network manager. Flow control, priority of service, and adding information concerning the logical connection is controlled here. The fifth layer is the session layer. It is the responsibility of the operating system and establishes user-to-user sessions. Headers to show the sender, receiver and packet sequence, and recovery are added here. The sixth layer is the presentation layer; where the system utilities break message into blocks and compress text. Finally, the seventh layer is the application layer, which is the responsibility of the user's program. This is where the messages that go over the network are initiated.

b. Encryption in Networks

The vulnerable points of the computer networks are obvious. Since the information flows through an open medium that is interceptible by the attacker, steps must

be taken to keep him from being able to read it once he intercepts it. There are two encryption schemes that can be used to conceal the plaintext from the intruder. They are link encryption and end-to-end encryption.

(1) Link encryption. It is performed in the low-level protocol layers (first and second layer). Data is encrypted just before it is placed on the physical communication link and the encryption process is invisible to user. Encryption protects the messages as they flow through the transmission media, but the messages are still in plaintext inside the hosts. This means that a message is vulnerable if it passes through a host that is not secure. It is most appropriate to use link encryption when the transmission line is the greatest point of vulnerability.

(2) End-to-End Encryption. It is performed in the highest layers (the sixth and seventh layers). Data is in encrypted form throughout the network and the user is involved in the encryption process. The messages are not in plaintext inside any of the intermediate hosts that they pass through. End-to-end encryption reduces the vulnerabilities when a message must be passed through several hosts, any of which may be insecure. It is most appropriate when untrusted systems may be attached to the network.

c. *Port Protection*

Port protection is used to prevent unauthorized access through the network to connected computer systems. The data flowing through a network is protected by network security which was described in the previous section. However, to prevent an unauthorized user accessing a computer system through the network, the data ports must be protected. The dial-in modem is an especially vulnerable point.

One kind of modem port protection is the automatic call-back. With this device, every time a user dials into the system the computer accepts the user ID and then breaks the phone connection. It then finds the approved phone number for that user and

calls the user back. When an unauthorized user dials into the computer system and identifies himself as an authorized user, the computer system will call the legitimate user instead of the unauthorized user. The disadvantage of this kind of protection is that a user can only dial into the computer from specific place, and special arrangements must be made for a user traveling with a portable computer.

Another kind of protection is differentiated access rights. Differentiated access rights limits the access to sensitive data when that access is attempted over a modem even though the user has access over a local terminal. To access the sensitive file, he or she must use an approved site.

Another protection is the silent modem. The silent modem does not answer an incoming call by sending carrier tone the way that a normal modem does, it waits for the initiating modem to send tone and then answers. In this manner, the modem does not identify itself as being a computer system until it is convinced that it is being called by another computer.

Finally, node authentication is used to authenticated other nodes on the network. With this kind of authentication scheme, no node will pass traffic to another node until that node has authenticated itself.

4. Multilevel Security Criteria

There are many kinds of multilevel security implemented differently by many of the countries that exploit computer system as a main resource in their information systems. Some of the multilevel security evaluation criteria produced by these countries are discussed here.

a. U.S. DoD Trusted Computer System Evaluation Criteria (TCSEC)

In 1983 the U.S Government published the DoD Trusted Computer System Evaluation Criteria (TCSEC), often referred to the "Orange Book." This book was first reviewed and republished in 1985, as DoD standard 5200.28-STD. [NCSC85, p. 7-50]

This document defines four(4) broad hierarchical divisions for the protection of computer systems. They are: D (minimal security), C (discretionary protection), B (mandatory protection), and A (verified protection). These broad criteria are further refined to reflect varying degrees of security within each divisions. Higher numbers within each divisions reflect greater security. The correct levels, in order of increasing levels of trust are as follows: [NCSC85, app. C and PFLE89, p.284 - 286]

(1) Class D: Minimal Protection. This class is reserved for systems that failed the evaluation. In fact no security characteristic is needed for this class.

(2) Class C1: Discretionary Security Protection. In this class, the minimum standard must satisfy the discretionary access control, and be implemented by the separation of users and data. The enforcement mechanism defined in this class specifies access limitation to control the data and allow the users to protect their own data. Identification and authentication are needed in this class. Users need to identify themselves to access the system and the system protects the authentication data.

(3) Class C2: Controlled Access Protection. The discretionary access control is enforced to a finer degree in this class than in class C1. Protection must be implemented to the single user level. In this class the object reuse policy is implemented so that the residue or unused object cannot be used by anyone else. In addition, an audit trail is required for this class so that all accesses or attempted accesses can be traced back to an individual.

(4) Class B1: Labelled Security Protection. The discretionary access control and object reuse is implemented in a similar fashion to the C2 class. In addition, the requirements of informal statement of security policy model, data labelling and mandatory access control over named subjects and objects are added. The labelling of exported information is required. Any flaws identified by testing must be removed.

(5) Class B2: Structured Protection. In this class the discretionary and mandatory access control policy enforcement methods mentioned in class B1 must be extended to all subjects and objects. The system must be divided into protection-critical and non-protection-critical sections. In addition the audit trail system, authentication mechanism and the trusted path must be strengthened. The design specification and implementation are subjected to extended testing and review. Covert channel analysis must be present. Trusted facility management is provided by support for system administration and operator functions, and configuration management controls are extended. This system is relatively resistant to penetration.

(6) Class B3: Security Domains. In class B3 the trusted recovery must be added to the required elements in B2. The discretionary access control, audit trail and trusted path are further enhanced and the system must satisfy the reference monitor requirements. The security functions must be tamperproof, and must be small enough for extensive testing and analysis. Significant system engineering during design and implementation are needed in order to minimize its complexity, i.e., using layering, abstraction and information hiding. This system is highly resistant to penetration.

(7) Class A1: Verified Design. In class A1, trusted distribution is added. Systems in this class are functional equivalents of the systems in class B3. The formal model design specification and verification in this system will result in a high degree of assurance. This system requires formal analysis of covert channels.

The "Orange Book" is recognized as first document to define multilevel security, and many countries have developed their evaluation criteria based on this book

b. The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)

The Canadian government recently established the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), however the complete document has not been published yet. Basically, this document is explained as the Canadian interpretation of U.S. DoD 5200.28-STD (TCSEC). [CSSC91, p. xi]

The document is divided into five (5) categories or levels; Confidentiality, Integrity, Availability, Accountability and Assurance. Compared to the "Orange Book," which is divide into four (4) groups or requirements: security policy, accountability, assurance, and documentation, CTCPEC addresses one of the criticisms of the "Orange Book." CTCPEC adds the area of insuring availability as a major component of computer security. The deeper levels of availability are not yet defined since this document is still in development.

Each category is split into classes and, similar to TCSEC, each of them is refined into varying levels. Confidentiality is split into four (4) classes: Discretionary (CD), Mandatory (CM), Partitions (CP) and Object Reuse (CR). Depending on the range, each class has a range level indicated by a number behind it, for example CD-1 is Confidentiality/Discretionary Protection level one (1). The range level varies for every class depending on the hierarchical base.

Compared to the groups of requirements in "Orange Book", the three classes in CTCPEC which are discretionary, mandatory and object reuse are interpretations of the security policy in the "Orange Book." The partitions class describes the compartments which address the labelling system in the security policy of the "Orange Book".

As with Confidentiality, Integrity is split into three (3) distinct classes: Discretionary Protection (Id), Mandatory Protection (IM), and Separation of Duties (IS); and each class has range levels. The basic structure of the integrity criteria is expected to follow that of the confidentiality criteria.

Furthermore, Accountability (describing "who") is split into 3 distinct classes: Identification and Authentication (WI), Audit (WA), and Trusted Path (WT). These criteria are drawn directly from the "Orange Book".

Finally, Assurance (another word for "trust") is one (1) class, and covers the range of: Operational Trust (TO), Life Cycle Trust (TL), and Documentation (TD). The assurance criteria are used to establish the degree to which evidential support and subsequent reasoning exists about how the chosen product's mechanisms and design will support the specified product security policy, throughout the life of the product. These assurance criteria are directly extracted from the TCSEC.

c. European Community Advisory Group Information Technology Security Evaluation Criteria (ITSEC)

The European Community advisory group developed the Information Security Evaluation Criteria (ITSEC), published in 1992. Currently, this book is known as "Europe's White Book." This book harmonized the criteria of France, Germany, the Netherlands, and the United Kingdom. Like the CTCPEC, this book also frequently referenced the U.S. TCSEC. In addition to the "White Book", the German Information Security Agency (Zentralstelle fur Sicherheit in der Informationstechnik) published Criteria for the Evaluation of trustworthiness of Information Systems in July 1989. At the same time France developed the same criteria in the so-called "Blue-White-Red Book" (SCSSI). The U.K. also produce a similar criteria for security evaluation.[SOGI91, p.9]

Basically the criteria define ten (10) distinct classes of security functionality which is based upon classes defined in the German National criteria, and seven (7) distinct classes of Assurance. [DITT91, p.269 and RUSS91, p. 319-321]

The ten (10) classes of security functionality are:

(1) F1: Discretionary Security Protection. This class is derived from "Orange Book" class C1.

(2) F2: Controlled Access Protection. This class is derived from "Orange Book" class C2.

(3) F3: Labelled Security Protection. This class is derived from "Orange Book" class B1.

(4) F4: Structured protection. This class is derived from "Orange Book" class B2.

(5) F5: Security Domains. This class is derived from "Orange Book" class B3/A1.

(6) F6: High Integrity for data and programs. A distinct class for systems with high integrity (in contrast to confidentiality) requirements for data and programs. It's particularly appropriate for database systems.

(7) F7: High Availability. A distinct class for systems with high standards for either a complete system or a special function of a system. It's particularly appropriate for process control systems.

(8) F8: High Integrity during data communication. A distinct class for systems with high standards for safeguarding data integrity during data communication.

(9) F9: High confidentiality during data communication. A distinct class for systems with high standards of confidentiality of data during data communication. It's particularly appropriate for cryptographic systems.

(10) F10: Networks with high demands on confidentiality and integrity. A distinct class for networks with high demands for the confidentiality and integrity of the information to be communicated. It's particularly appropriate when sensitive information needs to be communicated over insecure (e.g., public) networks.

And the seven (7) assurance levels are:

(1) E0: Inadequate confidence. Roughly equivalent to "Orange Book" class D assurance.

(2) E1: Tested. Roughly equivalent to "Orange Book" class C1 assurance.

(3) E2: Configuration control and controlled distribution. Roughly equivalent to "Orange Book" class C2 assurance.

(4) E3: Access to detailed design and source code. Roughly equivalent to "Orange Book" class B1 assurance.

(5) E4: Rigorous vulnerability analysis. Roughly equivalent to "Orange Book" class B2 assurance.

(6) E5: Demonstrates correspondence between detailed design and source code. Roughly equivalent to "Orange Book" class B3 assurance.

(7) E6: Formal models and formal descriptions, linked by formal correspondences. Roughly equivalent to "Orange Book" class A1 assurance.

d. U.K Technical Criteria for Security Evaluation

The U.K also developed the Technical Criteria for Security Evaluation which was published in February 1989. [DITT91, p. 268] This document specifies security functionality in two complementary ways:

(1) Security Prerequisites define a set of axiomatic statements about the properties required of a system to provide for maintenance.

(2) Claims Language defines a language that is used to describe the features in a form suitable for use as a standard for evaluation.

The Security prerequisites are categorized in two types: Security controls which are enforceable (X1 to X6), and Security objectives that are not enforceable (Y1 to Y5).

The enforceable security controls are:

(1) X1: Accountability

(2) X2: Authentication

(3) X3: Permission

(4) X4: Object Protection

(5) X5: Object Reuse

(6) X6: No Repudiation

And security objectives that are not enforceable are:

(1) Y1: No Addition

(2) Y2: No Loss

(3) Y3: Confinement

(4) Y4: Timeliness

(5) Y5: No Denial of Resources

A table inside this document is used to match the security claim phrase which is satisfied by each security prerequisites. From this, a matching evaluation level can be found as level from L1 to L6.

5. The Need for Multilevel Security

In the previous section, one method to ensure that computer system security works perfectly is data access control. The best known way to implement it is the multilevel security model. Multilevel security data bases require two or more levels of security for both the data elements and the users of one data base. [PFLE89, p. 329] Data in the system is segmented into parts that have their own classification, every user in this system also has his own level that indicates permission to access data. One example is the United States military security model. Every user in the system has a level of security, and the file has a level. The level of the user defines what kind of data level can be accessed. Subsection one (1) in this section described how the military models work.

If the Indonesian Navy is to complete every mission and task, it must continue to develop its information technology. Computers and communication networks move information around at the speed of light. The Navy began moving into the information age more that ten years ago with a stand-alone computer. They are now upgrading the communications infrastructure to support local and wide area networks.

Multilevel security offers the Navy the opportunity to protect the nation's secrets while keeping up with the demands for speed and reduced costs.

E. SUMMARY

The first problem in implementing a computer security system is identifying the threats to the computer system. This chapter described several threats to computer security; threats to the physical system, to the software, and to the data. The threats were also divided into internal or external threats. These threats are due to the system integrity,

privacy. Several controls to protect against these threats are also described in this chapter, as well as an approach to determining cost effectiveness. The next chapter reviews the current policies of the Indonesian Navy regarding computer security.

III. REVIEW AND CRITIQUE OF THE CURRENT COMPUTER SECURITY POLICY OF THE INDONESIAN NAVY

A. THE COMPUTER SYSTEMS USED BY THE INDONESIAN NAVY

The first computers procured by the Indonesian Navy were analog computers that were installed on war ships to calculate gun trajectories and control existing weapon systems. These computers controlled mechanical linkages and gears. The software was not susceptible to viruses because it was not able to generate corrupted copies of itself or other software. The only computer security required was physical security.

In the early 1970's the Indonesian Navy developed an information center to support more sophisticated general-purpose digital computers. The first system installed in the center was an International Business Machine (IBM) mainframe model 370. The primary uses were administrative, personnel management and payroll functions. Because of the centralized design and operation of early mainframe computers, security needs were limited to personnel security and physical security.

In the late 1970's the Indonesian Navy continued the modernization program by purchasing new ships. These ships were built and outfitted in Europe and included modern digital computerized weapon-control systems. These computer systems were built by HSA Holland, a subsidiary of Philips. The software used in this system was written or modified by HSA Holland at the time of manufacture and in accordance with the Indonesian Navy's specifications. Because of the real-time processing requirement, the systems were all coded in assembly language.

To promote standardization, the next order of ships used the same fire-control systems. To support these ships, the Navy expanded the computer center. They added a Digital Equipment Corporation (DEC) VAX-11/750 running VAX/VMS. The software

and hardware have been upgraded as needed and other facilities have been added, as the center outgrew its original building. At this point in the center's development, the computer systems were still isolated and physical and personnel security were all that was required.

The next step in the Navy's use of computers was the introduction of personal desktop systems to further support administrative and logistics functions. Because of Indonesia's poor quality telephone lines, the computers still operated in a stand-alone manner.

Now the Navy intends to install local-area networks as the first phase of a program to develope a data-communications network that will connect all the computer systems. This will greatly complicate the security requirements.

B. CURRENT POLICIES AND STANDARDS IN THE INDONESIAN NAVY

Naval Chief of Staff Regulation No. JUKNIK/6/VI/81, dated 20 June 1981, is the current regulation that establishes standards of information systems.

The regulation is a combination of reference material that was supplied by the manufacturers of the Navy's systems and literature that was found in other countries. The regulation focused on personnel threats from inside the organization because there were no known attempts at unauthorized access by hackers or spies. Threats to the data were perceived to come from the computer center personnel and were compensated for by organizational structure. Threats from outside the computer centers were nullified with physical security such as guards and locks.

Regulation No. JUKNIK/6/VI/81 defines four organizational responsibilities for every computer center and Navy office equipped with a computer system. They are:

1. Personnel security
2. Physical security

3. System development

4. Planning and operating security

In addition to the organizational responsibilities, there is great emphasis that every user is personally responsible for securing information.

1. Personnel Security

Personnel security requires that each person with access to a computer system must have a security clearance with a prescribed level of access. That person may then use the files that are at or below his or her access level. Prior to using a file with a higher access level, he or she must be granted clearance by the information security administrator. Even government officials are required to be granted access before being allowed to have the information in a computerized file. This restriction extends to the maintenance personnel. Maintenance personnel will either have a clearance and access to the highest level of information stored on the machine or they will be supervised at all times by personnel that do have the appropriate clearance and access.

2. Physical Security

The physical security requirements are the most precise because the threats are the most obvious and most predictable. The effect of natural disasters such as floods, storms, and fires can be predicted and mitigated through site location and construction standards, and this regulation has stated the common equipment and backups to be used against them.

Computer network security is also discussed in a global and theoretical manner, since the network itself was not completed at the time the regulation was written. Document security stresses the destruction of paper products and does not adequately address the control and destruction of electronic media such as disks and tape or electronic messages such as E-mail and electronically transferred files.

3. System Development

The section on system development addresses the need for standard procedures and documentation. Every program file should be validated and verified before it is accepted for use on the system. To record faults in the operation of the computer system the regulation specifies a log book or journal. The use of an automated journal that would automatically record discrepancies and report them to the system administrator and security administrator is not discussed. Therefore, the effectiveness of the recording and reporting system rely almost completely on the human operators. Individual ethics, morality and dependability are the major components of this critical reporting system.

4. Planning and Operating Security

The section concerning planning and operating system security specifies the required plans and procedures to ensure the secure use of the system. This includes instructions for authenticating and validating source data before entering it into the computer system. The use of cryptographic devices for protecting communications and data and the requirements for security checks of the communications channels are in this section. Also included are requirements for equipment layouts to ensure such things as the placement of terminals to prevent viewing by unauthorized personnel.

System security includes file access, hardware integrity, and software integrity. File access is controlled by passwords, badge reading, assigning file attributes such as read, write and execute to each individual, and even by limiting access to certain files to specific terminal addresses. The regulation specifies regular and as-needed changes of passwords and badges to maintain security.

Maintaining hardware integrity is essential for the secure operation of a computer system. The regulation mentions several methods for ensuring aspects of hardware integrity. They include read after write, parity checks, check sums, check digits,

hash and counts, and sequence numbers. All these methods will verify some aspect of system integrity. But along with adding to the cost of the computer system, security devices in the hardware impact the computer performance. [LANE85, p. 55] There is very little discussion in the regulation of how to determine the effective trade-off between cost, performance, and security.

This section also lists several requirements to insure software integrity, but it is very unclear what the original author or authors were trying to accomplish. The regulation states that violations of software integrity can be detected by observing the file number and by automatically verifying the programs code. Unauthorized variations in the code or the file number indicate a violation. The program must be prevented from losing, corrupting, or copying data. The operating system must be capable of controlling the data transfer between the processor and on-line devices, fully protect the memory, and be able to interrupt system and peripheral devices as needed. It should also be able to limit access of maintenance personnel to authorized levels and procedures. And the erasure of classified information must be conducted and verified in such a manner that there is no residue. This section must be rewritten to clarify the instructions as well as to reflect current technology.

5. Personal Responsibility

Finally, the regulation stresses the individual user's responsibilities concerning information security. These responsibilities are stressed as an ethical issue instead of a regulatory issue. Security depends on every person who uses the information bearing in mind that the information is to be used for the good of all Indonesians. When that occurs, all are aware of the meaning of security and how important it is.

C. THE POLICY NEEDS TO BE UPDATED

There are many reasons that the polices and standards now used by the Indonesian Navy need to be updated. The most obvious reason is that technology has changed so much. Since Regulation No. JUKNIK/6/VI/81 was written in 1981, the regulation has become obsolete. The techniques of hackers, crackers and spies have kept pace with the advances in technology and the Navy will be vulnerable until its security regulations and security programs recognize and deal with these threats. Several matters that are inadequately addressed or not addressed at all are:

1. The Proliferation Of Viruses, Trojan Horses, And Worms

There is no definite time when the term computer virus was coined, but the day when Dr. Frederick Cohen published his thesis about computer viruses (1984), seems to mark the first published reference. At least his thesis marks the time when the treat of viruses began to be explored by computer scientists. Since the regulation was written three years before Dr. Cohen's thesis, the work on this kind of program sabotage needs to be included.

2. Powerful Personal Computers Are Becoming Widely Available

With the proliferation of powerful personal computers available at modest prices, it is becoming more common for professionals to have a computer to work on at home. Since these computers are not subject to the same protections as the ones in the office, they can be the source of infections and attacks. The regulation must deal with persons moving files between their systems at home and their systems at the office.

3. Networked And Distributed Processing Systems

As the telecommunications systems are improved, computer networks and distributed computing systems will become more prevalent. Because the number of entry

points for an attacker is increased, the controls are harder to implement. A major problem for commanders and administrators is that for the first time terminals and systems that can be the source of an attack on their systems are not under their control. Thus, for them to have confidence in their security, they must believe that all systems security on the network is the same. This is easiest to accomplish by placing the requirements in a regulation that applies to all organizations on the network.

4. Rapid Technological Development

The technology of computer security has developed quite rapidly in industrialized nations as a result of miscellaneous attacks on their systems. Indonesia, as a developing country, can be a purchaser of much of this computer security technology. Security regulations must make provisions for the on-going review of technological developments and their insertion into the Navy's systems.

5. Increasing Reliance On Computer Systems For National Security

The primary task of the Indonesian Navy is defense of Indonesia from possible attacks. Because the Navy is relying more and more on computer systems to accomplish its missions, the effect of a successful attack on the computer systems is becoming ever more serious. The regulation must provide guidance to all levels of administration for protecting against this threat.

6. Multi Level Security (MLS)

Regulation No JUKNIK/6/VI/81 was written prior to the public discussion of multilevel security (MLS), so it does not include any reference to the concept. MLS has many advantages in terms of cost savings and reduced overhead. Because all information can exist on one system regardless of security classification, redundant systems do not have to be purchased, installed and administered. Databases do not have to be replicated and

maintained on multiple systems and more efficient use can be made of all equipment. The potential savings are immense. MLS will be an important component of the next security regulation.

D. SUMMARY

This chapter reviewed the current computer security policy of the Indonesian Navy which is implemented in Naval Chief of Staff Regulation No. JUKNIK/6/VI/81, dated 20 June 1981. The regulation codifies the policy governing computer security in the late seventies. Due to advances in computer technology, the infrastructure that supports it, and our growing reliance on computer systems, new policies are needed to ensure that those systems are available when we want to use them. The next chapter proposes changes to Indonesia's existing policies to reflect current technological advance.

IV. POLICY FOR THE INDONESIAN NAVY

Having studied the foundational concepts of computer security and reviewing the existing regulations about computer security in the Indonesian Navy, we can now determine what actions are required to improve the policy that is already in place.

A. THE NEED FOR A COMPUTER SECURITY POLICY

The goal of developing a policy on computer security is to define the organization's expectations of proper computer and network use and to define procedures to prevent and respond to security incidents. In order to do this, aspects of the particular organization should be considered.

Since this policy is developed for the Indonesian Navy, the organizational goals concern the safety and unity of the whole nation. To achieve these goals of national security, computer security must be a top priority of all users of computer systems. However, not all information in the Indonesian Navy can be considered top secret, some of it may be secret, confidential or even unclassified. Thus, the most effective system to have is a multilevel security (MLS) system.

However, since the implementation of a multilevel security system is costly, and since some systems now owned by the Indonesian Navy are still useful, the policy must address an evaluation criteria that evaluates existing as well as proposed systems. In this manner, the machines that fail the evaluation for processing a certain classification of information may still be used to process information at a lower classification.

The second function of the evaluation criteria will be to assess the suitability of proposed equipment. Using the criteria will aide the security and acquisition personnel insure that new systems and components support the approved security architecture.

1. Policy Maker Responsibility

Policy creation must be a joint effort by technical personnel, who understand the full ramifications of the proposed policy and the implementation of the policy, and the decision makers who have the power to enforce the policy. A policy that is neither implementable nor enforceable is useless.

In the Indonesian Navy, the policy should be established by the joint effort of the Naval Data Collection and Information System, Naval Telecommunication and Electronic Directorate, Naval Sensor, Weapon and Command Directorate as the technical personnel, and Naval Security Directorate, and Naval Operation Directorate as the decision maker who enforce the policy.

Furthermore, the directorates mentioned above will have their own responsibilities in the security organization form for computer system.

2. Evaluation Criteria as the First Step

Chapter III described some of the old models of computer systems adopted by the Indonesian Navy. As a developing country, establishing a new system by discarding an existing system is a very costly action, especially if computer production is dependent on a foreign country.

To avoid spending money for replacing every computing system with new equipment to exactly implement the multilevel security, the existing equipment may be used for a lower classification of information. An evaluation criteria is needed in order to define the classification of existing equipment. Certain levels of information may be kept or processed on these older systems based on the classification of the equipment.

In addition, this evaluation guide will be used to develop a new system or purchase an available system to be used by the Navy to support any tasks that are suitable

for automation. It is clear that the Navy needs a new guide. The next task is to choose the published criteria that is the most applicable to the Navy's requirements.

B. THE NEEDS OF THE INDONESIAN NAVY

The first published criteria for evaluating multilevel security systems is the Trusted Computer System Evaluation Criteria developed by the U.S. Government. Using this guide as a baseline, other countries developed evaluation criteria of their own. They are Canada, Germany, the U.K., the Netherlands, France, Australia and New Zealand. Germany, the U.K., the Netherlands and France went on to develop a harmonized criteria for the European Community.

1. Criteria for the Indonesian Navy

Indonesia needs to have an evaluation criteria for the computer systems that are already installed as well as those that they will procure in the future. The Indonesian Navy, as a military organization, exploits computer systems to support its operations. Since the Navy is a complex organization with different classification levels of information, they will benefit from a multilevel security criteria.

The Indonesian Navy imports all of the hardware and software that it uses. As a consequence, the criteria they adopt should match the machines being imported. The mainframe computer systems are mainly imported from the U.S., and personal computers are imported from Asian countries. So, it is important that the first evaluation criteria should refer to the U.S. products. In other words, they should adopt a policy based on the "Orange Book."

However, the "Orange Book" from the U.S. Government must be supported by the rainbow series, which is too large and complicated to be adopted by the Navy at this time. Currently, the information technology and the infrastructure possessed by the Indonesian Navy does not require this complicated approach.

The ITSEC from European Community are not straight-forward evaluation criteria, but depend on the technical judgements of experts in each country. This occurred because the ITSEC is a harmonized criteria from several countries in Europe. This would be difficult for the Indonesian Navy to adopt because they do not have the experts to interpret the ITSEC.

The Canadian Government directly interprets the "Orange Book" in the Canadian Trusted Computer Product Evaluation Criteria. It is a simple publication and, with small modifications, can be adapted to the Indonesian Navy.

The purposes of the recommended Trusted Evaluation Guide (TEG) which is adapted from Canadian Trusted Computer Product Evaluation Criteria are:

a. Measurement

To provide Indonesian Navy with a metric with which to evaluate the degree of trust that can be placed in computer products used for processing of sensitive information.

b. Guidance

To provide a guide to contractors/manufacturers as to what security features to build into their new and planned, commercial products in order to produce widely available products that satisfy trust requirements for sensitive applications.

In Chapter II it was noted that the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) is divided into five categories or levels; Confidentiality, Integrity, Availability, Accountability and Assurance. The recommended Trusted Evaluation Guide is also divided in the same way; a detailed description of each of these areas can be found in section D of the appendix.

Since many documents refer to the U.S. Trusted Computer System Evaluation Criteria (TCSEC), it is useful to provide a mapping of the classes found in the recommended Trusted Evaluation Guide (TEG) for the Indonesian Navy to those found in the TCSEC.

a. ***Confidentiality mappings:***

Confidentiality/Discretionary Protection:

TEG	**TCSEC**
CD0	D1
CD1	C1
CD2	C2 - B2
CD3	B3 - A1

Confidentiality/Mandatory Protection:

TEG	**TCSEC**
CM0	D - C2
CM1	B1
CM2	B2
CM3	B3 - A1

Confidentiality/Partitions:

TEG	**TCSEC**
CP0	D - C2
CP1	not available
CP2	B2 - B1
CP3	B3 - A1

Confidentiality/Object Reuse:

TEG	TCSEC
CR0	D - C1
CR1	C2 - A1

b. Integrity mappings:

Integrity/Discretionary Protection:

TEG	TCSEC
ID0	D - A1

Integrity/Mandatory Protection:

TEG	TCSEC
IM0	to D - A1

Integrity/Separation of Duties:

TEG	TCSEC
IS0	D
IS1	C1 - C2
IS2	B1 - B2
IS3	B3 - A1
IS4	not available

c. *Accountability (Who) mappings:*

Accountability/Identification and Authentication:

TEG	TCSEC
WI0	D
WI1	C1
WI2	C2
WI3	B1 - A1

Accountability/Audit:

TEG	TCSEC
WA0	D - C1
WA1	C2
WA2	B1
WA3	B2
WA4	B3 - A1

Accountability/Trusted Path:

TEG	TCSEC
WT0	D - B1
WT1	B2
WT3	B3 - A1

d. Assurance (Trust) mappings:

Assurance/Operational Trust:

TEG	TCSEC
TO0	D
TO1	C1
TO2	C2
TO3	B1
TO4	B2
TO5	B3
TO6	A1

Assurance/Life Cycle Trust:

TEG	TCSEC
TL0	D
TL1	C1
TL2	C2
TL3	B1
TL4	B2
TL5	B3
TL6	A1

Assurance/Documentation:

TEG	TCSEC
TD0	D
TD1	C1
TD2	C2
TD3	B1
TD4	B2
TD5	B3
TD6	A1

From this mapping, it is clear that there is a close correspondence between the proposed Trusted Evaluation Guide (TEG) and the U.S. TCSEC, which may aid in performing cost effective evaluations of systems.

2. Security Organization

It was mentioned in Chapter II that individual users play the primary role in information security. However, there is a need for a formal executive body that is responsible for the computer security organization. In the Indonesian Navy, existing executive bodies may be assigned additional responsibilities concerning computer security.

The Naval Data Collection and Information System, as the incubator for information systems in the Navy, will be given the main responsibility for securing information systems. It will also act as the administrator that executes the regulation concerning computer systems. This body has the Navy's experts in computer technology.

The Naval Telecommunication and Electronic Directorate will be responsible for securing the computer network. In this body there is a special section that works with the

encryption and decryption techniques. With this experience, it can direct the use of encryption and decryption in the computer systems.

The Naval Sensor, Weapon, and Command Directorate is responsible for the combat information systems on board the ships. This information concerns combat information and is considered top secret. This body must clearly understand the value of information, and how to secure it.

All the organizations listed above have responsibilities in the technical areas of computer security. In order to enforce the security regulations, the executive body, which has the power to enforce the regulations, must be involved.

The Naval Security Directorate has primary responsibility in all aspects of security in the Navy. Therefore, it has responsibility for computer security as well. It will inspect the implementation of security in all of the Naval organizations that possess computer systems. This directorate needs to create a section with the primary responsibility for computer security policy and inspections.

The Naval Operations Directorate, as the top management level, has the power and responsibility to see that the security regulation is implemented thoroughly.

C. SUMMARY

An effective computer security policy supports the goals and missions of the organization. The goals and missions of the Indonesian Navy is nothing less than preserving the security and unity of Indonesia. Computer systems will continue to grow in importance as a tool for accomplishing those missions. An effective security evaluation program is essential to guarantee that the tool will be available when needed. The criteria to support such a program was laid out in this chapter. The next chapter contains the recommendations to implement an effective security program.

V. CONCLUSIONS AND RECOMMENDATIONS

Having studied the concept of ideal computer security and reviewed what has been done by the Indonesian Navy, it is obvious that the computer security regulation needs to be updated. This is especially true for the sections dealing with physical and communications security as well as data security, integrity and availability.

There are several actions that the Indonesian Navy needs to take to improve its computer security posture. Some actions should be taken immediately, some policies and procedures will take 12 to 18 months to develop and implement, while others will take many years. These recommendations are explained below.

A. REGULATIONS CONCERNING PHYSICAL SECURITY

There is a need to more clearly state the security requirements in Regulation No. JUKNIK/6/VI/81. The advanced technology available today can be applied to the physical security of computer systems. The amount and sophistication of the technology used should be balanced by the amount and value of the information in the system. For example, to protect an area where top secret information is processed may require sophisticated authentication devices such a magnetic stripe cards or a retinal pattern reader.

B. REGULATIONS CONCERNING DATA SECURITY, INTEGRITY AND AVAILABILITY

The regulations concerning data security need to be updated to reflect the developments in information technology. The networked and distributed computing systems are already being installed in the headquarters, starting with a local area network.

Obviously, with this development, the threats to data security, integrity and availability become greater. The regulation should be clearly written to cover these increased threats.

Regulations concerning virus protection also need to be written, since the Regulation No. JUKNIK/6/VI/81 was written before viruses were known. This is very important since the environment in Indonesia is so favorable for spreading viruses from one computer to another.

The Indonesian Navy needs to protect its systems with antivirus programs and procedures. The programs need to be updated regularly, because new and more sophisticated viruses are being developed all the time. A connection with an antivirus software manufacturer is recommended, so that, every product update is immediately available.

Until then, messages should be sent to all organizations using computer systems prohibiting disks that were used on nongovernment computers from being used on government computers.

C. RECOMMENDED TRUSTED EVALUATION GUIDE

As a military organization that has several degrees of information sensitivity, the Indonesian Navy needs to implement multilevel security (MLS), in certain critical areas that deal with classified information.

The recommended Trusted Evaluation Guide proposed for the Indonesian Navy in the appendix is adapted from the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) with minor modifications. This is because the CTCPEC is such a clear and simplified interpretation of the "Orange Book." The "Orange Book" requires the entire rainbow series, which is more than the Indonesian Navy requires at this time.

1. Intermediate Actions

The evaluation guide proposed in this thesis is not yet complete. The chapter covering data availability still needs to be written in order to have a complete definition of security. Furthermore, this evaluation needs to be expand in scope so that products from all over the world can be evaluated, since Indonesia may import systems from all over the world.

When the evaluation guide is completed and adopted, a trusted computing architecture must be developed that will guide all computer purchases for the Navy.

All communications links will be analyzed and prioritized by risk and the most vulnerable links will be encrypted and funds are make available.

2. Long Term Actions

The evaluation guide should be automated so that it will accelerate and simplify evaluations. A software system that accepts characteristic values of a system and automatically produces the required classification based on the evaluation guide will produce consistent results very quickly. This will increase use of the evaluation criteria and possibly reduce the time it will take to achieve a trusted network. In a nonautomated system for conducting evaluations, several highly skilled individuals are required. Automation is highly recommended since the Indonesian Navy currently possesses few experts with the required skills to perform evaluations.

In addition, the U.S. Federal Government together with Canadian Government are developing joint standards in evaluating a computer products. These actions may be followed by harmonization with European countries. The proposed Trusted Evaluation Guide positions Indonesia to participate in these efforts.

As trusted systems and components are procured, they will replace the untrusted systems currently in use.This will strengthen the entire security posture of the Indonesian

Navy. But, empirical and validation studies that measure the effect of the statements in the evaluation guide is needed.

D. SUMMARY

Taking these steps will enable the Navy to plug many of the most dangerous holes immediately, design a balanced security program in the near future, and build a trusted multilevel computing environment over time. In the end, the Indonesian Navy will have a security system that is versatile, effective, and efficient. This is a goal well worth working towards.

APPENDIX

RECOMMENDED TRUSTED EVALUATION GUIDE

I.INTRODUCTION

A. HISTORICAL PERSPECTIVE

The criteria presented in this document are based on the U.S. Department of Defense Trusted Computer System Evaluation Criteria (DoD 5200.28-STD) which evolved from the earlier NIST, and MITRE evaluation material.

B. SCOPE

The trusted computer product evaluation criteria defined in this document apply primarily to trusted, commercially available electronic data processing (EDP) products.

Included are two distinct sets of requirements:

1. Specific Security Feature Requirements

The specific feature requirements encompass the capabilities typically found in information processing products employing general-purpose operating systems that are distinct from application programs being supported. However, specific security feature requirements may also apply to specific products with their own functional requirements, applications or special environments (e.g. communications processors, process control computers, and embedded products in general).

2. Assurance Requirements

The assurance requirements, on the other hand, apply to products that cover the full range of computing environments from dedicated controllers to full range multilevel secure resource sharing products.

C. PURPOSE

The criteria have been developed to serve a number of intended purposes:

1. To provide the Indonesian Navy with a metric with which to evaluate the degree of trust that can be placed in computer products used for the processing of sensitive information; and

2. To provide a guide to manufacturers as to what security features to build into their new and planned, commercial products in order to produce widely available products that satisfy trust requirements for sensitive applications.

With respect to the first purpose for the development of criteria, i.e., providing the Indonesian Navy with a security evaluation scale, evaluations can be delineated into two types:

1. An evaluation can be performed on a computer product from a perspective that excludes consideration of a specific application environment.

2. An assessment can be done to determine whether appropriate security measures have been taken or can be taken to permit the product to be used operationally in a specific application environment. This type of evaluation is more commonly known as a risk assessment.

It must be understood that the completion of the first type of evaluation, i.e., a formal product evaluation under the Trusted Product Evaluation Program, does not constitute certification approval for the product to be used in any specific application environment. The evaluation report only provides a trusted computer product's strengths and

weaknesses from a computer security point of view. A risk assessment and the formal approval, done in accordance with the applicable policies of the Indonesian Navy and of the institution(s) which intend to use the product, must still be followed before a product can be approved for use in processing or handling classified information in a particular application. Directorate Security remains ultimately responsible for specifying the security requirements for their respective EDP systems.

The trusted computer product evaluation criteria will be used directly and indirectly in the certification and approval processes. The criteria will be used directly as technical guidance for evaluation of a product being considered for certification and for specifying certification requirements for such a product. Where a candidate product being evaluated for certification employs, as a subsystem, another product that has already undergone an evaluation under the Trusted Product evaluation Program, reports from the evaluation of the subsystem will be used as input to the evaluation of the candidate product. The criteria will be used indirectly, as reference, during the risk assessment process.

Technical data will be furnished to designers, evaluators and Directorate Security to support their needs for making decisions.

D. FUNDAMENTAL COMPUTER SECURITY REQUIREMENTS

Any discussion of computer security necessarily starts from a statement of requirements, i.e., what really means to call a computer product "secure". In general, a secure product will control, through use of specific security features, access to information within the control of the product such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, create, or delete information. Figure 1 graphically illustrated the basic thought of the basic structure of a "secure" system. Six fundamental requirements are derived from this basic statement objective: four deal with what needs to be provided to control access to information; and

two deal with how one can obtain credible assurances that this is accomplished in a trusted computer product.

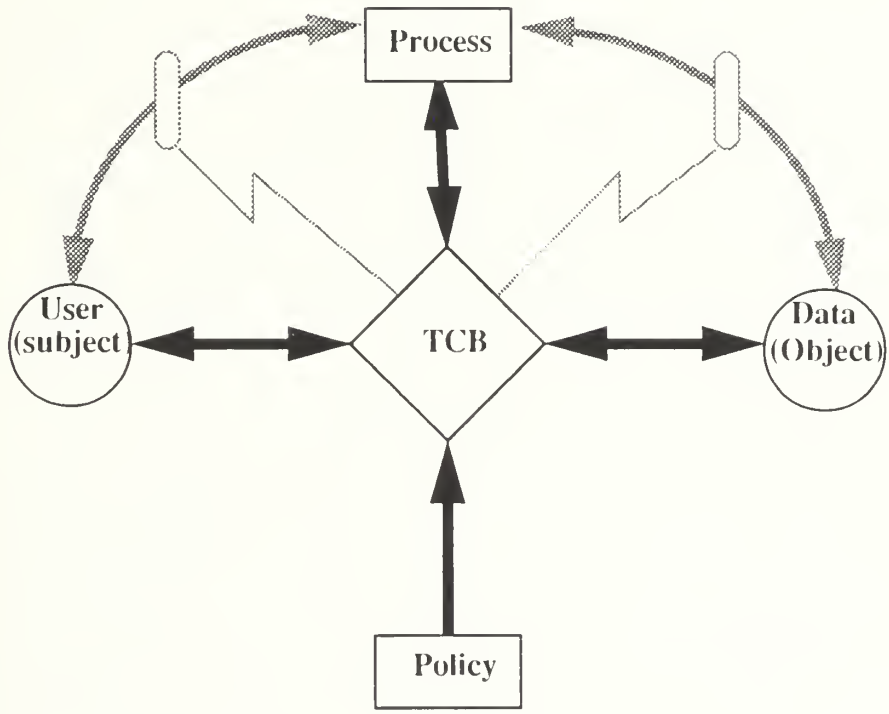

Figure 1 View of a Secure System

1. Subjects, objects, and Processes as "Entities"

Unlike the traditional view of subjects and objects espoused by the NCSC, this Recommended Trusted Evaluation Guide's view of each is isomorphic.

To view each entity one must view it from the perspective of the TCB. In this way one can see that each entity is an entity with at least the following attributes:

a. Name

What is the name of the entity (i.e., user ID, name of file, etc.)

b. Label

Designated level of operation. This is set at login time for subjects, and known for processes and objects.

c. Multilevel

Is the entity capable of multilevel access?

d. Discretionary Access Restrictions

What are the discretionary access restrictions to the entity?

e. Duty list

What are the entity's predefined duties?

This creates an isomorphic set of entities (Subject (User), Process, Data (Object)) which are accessed in an orthogonal way.The methods of access for objects are identical to those for subjects and processes. This allows for users to be viewed as multilevel devices as are most input/output devices. Also, a user would log in with a specific label associated with himself. This label would, to the TCB, look identical to labels associated with various objects and process throughout the system.

2. Security Policy

There must be an explicit security policy enforced by the product. This policy would consist at least one of: confidentiality, integrity, availability, and accountability. A level of assurance would be determined relative to the strength of the mechanisms within the product enforcing the security policy.

3. Confidentiality

a. Requirement 1: Discretion

Given identified subjects and objects, there must be a set of rules that are used by the product to determine whether a given subject can be permitted to gain access to a specific object.

b. Requirement 2: Compartmentalization

Given well defined compartments, be they hierarchical or not, the product must be able to determine the compartment at which the subject is working and the level of the object to which the subject wishes access and authorize (or not) access to the object according to the defined security policy of the product.

c. Requirement 3: Marking

Confidentiality labels must be associated with objects. In order to control operations on access to information stored in a computer, according to the rules of a mandatory security policy, it must be possible to mark every object with a label that reliably identifies the object's sensitivity level (e.g. classification, area of work, etc.) and/or the process authorization accorded those subjects who may potentially access the object.

4. Integrity

a. Requirement 4: Separation of Duties

Given well defined duties, the product shall ensure that any subject's attempt to access an object is properly authorized as defined by the security policy. Any attempt to access an object other than by a known path will be disallowed and appropriately recorded.

5. Availability (Not Yet Complete)

6. Accountability

a. Requirement 5: Identification

Individual subjects must be identified. Each access to information must be mediated based on who is accessing the information and what classes of information they are authorized to deal with. This identification and authorization information must be securely maintained by the computer product and be associated with every active element that performs some security-relevant action in the product.

b. Requirement 6: Accountability

Audit information must be selectively kept and protected so that portions of the audit record reflecting a security breach can be used to track down the responsibility party. A trusted product must be able to record the occurrences of security-relevant events in an audit log. The capability to select the audit events to be recorded is necessary to minimize the expense of auditing and to allow efficient analysis. Audit data must be protected from modification and unauthorized destruction to permit detection and after-the -fact investigations of security violations.

7. Assurance

a. Requirement 7: Assurance

The computer product must contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the product enforces requirements one through six above. In order to assure that the six requirements of Security Policy, Marking, Identification, and Accountability are enforced by a computer product, there must be some identified and unified collection of hardware and software controls that perform those functions. These mechanisms are typically embedded in the

operating system and are designed to carry out the assigned tasks in a secure manner. The basis for trusting such product mechanisms in their operational setting must be clearly documented such that it is possible to independently examine the evidence to evaluate their sufficiency.

b. *Requirement 8: Continuous Protection*

The trusted mechanisms that enforce these fundamental requirements must be continuously protected against tampering and/or unauthorized changes. No computer product can be considered truly secure if the basic hardware and software mechanisms that enforce the security policy are themselves subject to unauthorized modification or subversion. The continuous protection requirement has direct implications throughout the computer product's life-cycle.

E. STRUCTURE OF THE DOCUMENT

This document is divided into six parts. The first part covers the introduction, and the following five parts present the detailed criteria which relate to the fundamental requirements described above.

F. STRUCTURE OF THE CRITERIA

The criteria are divided into five categories: Confidentiality, Integrity, Availability, Accountability, and Assurance. Each category contains classes which are generally ordered in a hierarchical manner with the highest division being reserved for products providing the most comprehensive security features. Each division and class represents a major improvement in the features or assurance one can place in the product for the protection of sensitive information.

As improvements in the features are exposed within each of the five categories a level is assigned. This level, increases as the features increase. Each category is numbered

following a logical and linear path commencing at zero (0) and working upwards. Readers should not make the mistake of assuming that the levels of one category directly correlate to those of another. Although two levels within two distinct categories may be numbered the same they do not necessarily define a classification hierarchy. If one views the document as a set of five distinct criteria which are coupled by way of a constraint, one will have a better understanding of the structure. The breadth of Levels found within each category is defined below:

Confidentiality: Confidentiality is split into four distinct classes: Discretionary, Mandatory, Partitions, and Object Reuse. Each of these Classes have a range of levels:

Confidentiality/Discretionary Protection:	CD 0 - CD 3
Confidentiality/Mandatory Protection:	CM 0 - CM 3
Confidentiality/Partitions:	CP 0 - CP 4
Confidentiality/Object Re-use:	CR 0 - CR 1

Integrity: Integrity is split into three distinct classes: Discretionary, Mandatory, and Separation of Duties. Each of these Classes have a range of levels:

Integrity/Discretionary Protection:	ID 0 - ID 3
Integrity/Mandatory Protection:	IM 0 - IM 3
Integrity/Separation-of-Duties:	IS 0 - IS 4

Availability: Unknown at the present time.

Accountability:	Accountability is split into three distinct classes: Identification and Authentication, Audit, and Trusted Path. Each of these Classes have a range of levels:	
	Accountability/Identification & Authentication:	WI 0 - WI 3
	Accountability/Audit:	WA 0 - WA 3
	Accountability/Trusted Path:	WT 0 - WT 2
Assurance:	Assurance is one class. This class covers the following range:	
	Assurance/Operational Trust:	TO 0 - TO 6
	Assurance/Life Cycle Trust:	TL 0 - TL 6
	Assurance/Documentation:	TD 0 - TD 6

II.CONFIDENTIALITY

Confidentiality is broken down into constituent components. Each component describes a distinct and separate portion of the whole we call Confidentiality. These components are: discretionary protection, mandatory protection, partitions, and object reuse.

A. DISCRETIONARY PROTECTION

Levels within this division provide for discretionary protection at the control of the owner.

1. Level CD-0: Noncompliant

This level, Confidentiality/Discretionary Protection Level 0 (CD-0) is reserved for those products which have been evaluated but fail to meet the requirements of any of the Discretionary Protection required by confidentiality.

2. Level CD-1: Discretionary Security Protection

A confidentiality/Discretionary Protection Level 1 (CD-1) system nominally satisfies discretionary protection requirements by providing separations of users and data. It incorporates some form of credible controls capable of enforcing access limitations on an individual basis, i.e., suitable for allowing users to be able to protect private information and to keep other users from accidentally reading or destroying their data. The CD-1 environment is expected to be one of cooperating users processing data at the same level(s) of sensitivity.

The product shall define and control access between named users and named objects (e.g., files and programs). The enforcement mechanism shall allow users to

specify and control sharing of named objects by named individuals or defined groups of named individuals or both.

3. Level CD-2: Controlled Access Protection

Confidentiality/Discretionary Protection Level 2 (henceforth CD-2) products enforce a more finely grained discretionary protection than CD-1 products and provide a limited form of resource isolation.

The product protection mechanisms shall define and control access between named users and named objects (e.g., files and programs). The enforcement mechanism shall allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. The discretionary protection mechanism shall provide that objects are protected from unauthorized access. This protection shall be capable of including or excluding access to granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

4. Level CD-3: Enhanced Controlled Access Protection

Confidentiality/Discretionary Protection Level 3 (henceforth CD-3) products enforce a more finely grained discretionary protection and provide a much stronger form of resource isolation than CD-2 products.

The product protection mechanisms shall define and control access between named users and named objects (e.g., files and programs) in the EDP system. The enforcement mechanism shall allow users to specify and control sharing of those objects and shall provide controls to limit propagation of access rights. The discretionary protection mechanism shall provide that objects are protected from unauthorized access. This protection shall be capable of specifying, for each such named object, a list of named individuals and a list of groups of named individuals with their respective modes of access

to that object. Furthermore, for each such named object, it shall be possible to specify a list of named individuals and a list of groups of named individuals for which no access is to be given. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

B. MANDATORY PROTECTION

Products in this division must include mechanisms which use labels to enforce a set of mandatory protection rules. The labels must be associated with all objects in the product. The system developer must provide the security policy model on which the protection mechanisms are based and must furnish a specification for the protection mechanisms.

1. Level CM-0: Noncompliant

This level, Confidentiality/Mandatory Protection Level 0 (CM-0) is reserved for those products which have been evaluated but fail to meet the requirements of any of the Mandatory Protection required by confidentiality.

2. Level CM-1: Labelled Security Protection

An informal statement of the security policy model, data labelling, and mandatory protection over named subjects and objects must be provided. The capability must exist for accurately labelling exported information.

a. Labels

Labels associated with each subject and storage object under its control (e.g., process, file, segment, device) shall be maintained by the TCB. These labels shall be used as the basis for mandatory protection decisions. In order to import non-labelled data, the TCB shall request and receive from an authorized user the label of the data, and all such actions shall be auditable by the TCB.

(1) Label Accuracy. Labels shall accurately represent the sensitivity of the specific subjects or objects with which they are associated. When exported by the TCB, labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported.

(2) Exportation of Labelled Information. The TCB shall designate each communication channel and I/O device as either single-level or multilevel. Any change in this designation shall be done manually. The TCB shall maintain any change in the label associated with a communication channel or I/O device.

(a) Exportation to Multilevel Devices. When TCB exports an object to a multilevel I/O device, the label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When TCB exports or imports an object over a multilevel communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the labels and the associated information that is sent or received.

(b) Exportation to Single-level Devices. Single-level I/O devices and single-level communication channels are not required to maintain the labels of the information they process. However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the label of information imported or exported via single-level communication channels or I/O devices.

(c) Labelling Human-Readable Output. The EDP system administrator shall be able to specify the printable label names associated with exported labels. The TCB shall mark the beginning and end of all human-readable paged, hardcopy output (e.g., line printer output) with human-readable labels that properly represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human

readable, paged hardcopy output (e.g., line printer output) with human-readable labels that properly represent the overall sensitivity of the output or that properly represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable labels that properly represent the sensitivity of the output.

3. Level CM-2: Structured Protection

In Confidentiality/Mandatory Protection Level 2 (CM-2) systems, the TCB is based on a clearly defined and documented formal security policy model that requires the mandatory protection enforcement found in CM-1 systems to be extended to all subjects and objects in the EDP system. The TCB must be carefully structured into protection-critical elements.

a. Labels

Sensitivity labels associated with each EDP system resource (e.g., subject, storage object, ROM) that is directly or indirectly accessible by subject external to the TCB shall be maintained by the TCB. These labels shall be used as the basis for mandatory protection decisions. In order to import non-labelled data, the TCB shall request and receive from an authorized user the sensitivity level of the data, and all such actions shall be auditable by the TCB.

(1) Label Accuracy. Sensitivity labels shall accurately represent the sensitivity of the specific subjects or objects with which they are associated. When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported.

(2) Exportation of Labelled Information. The TCB shall specify each communication channel and I/O device as either single-level or multilevel. Any change in

this designation shall be done manually. The TCB shall maintain any change in the sensitivity levels associated with a communication channel or I/O device.

(a) Exportation to Multilevel Devices. When TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When TCB exports or imports an object over a multilevel communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the labels and the associated information that is sent or received.

(b) Exportation to Single-level Devices. Single-level I/O devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process. However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the sensitivity of information imported or exported via single-level communication channels or I/O devices.

(c) Labelling Human-Readable Output. The EDP system administrator shall be able to specify the printable label names associated with exported labels. The TCB shall mark the beginning and end of all human-readable paged, hardcopy output (e.g., line printer output) with human-readable labels that properly represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page with human-readable sensitivity labels that properly represent the overall sensitivity of the output or that properly represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB.

(3) Subject Sensitivity Labels. The TCB shall immediately notify a terminal user of each change in the sensitivity associated with that user during an interactive session. A terminal user shall be able to query the TCB as desired for a display of the subject's complete sensitivity label.

(4) Device Labels. The TCB shall support the assignment of minimum and maximum sensitivity to all attached physical devices. These sensitivity shall be used by the TCB to enforce constraint imposed by the physical environments in which the devices are located.

4. Level CM-3: Security Domains

The Confidentiality/Mandatory Protection Level 3 (CM-3) TCB must satisfy the reference monitor requirements that it mediate all accesses of subjects to objects, be tamper-proof, and be small enough to be subjected to analysis and test. To this end, the TCB is structured to exclude code not essential to security policy enforcement, with significant system engineering during TCB design and implementation directed toward minimizing its complexity. A security administrator is supported, audit mechanisms are expanded to signal security-relevant events, and system recovery procedures are required. The system is highly resistant to penetration.

a. Labels

Sensitivity labels associated with each EDP system resource (e.g., subject, storage object, ROM) that is directly or indirectly accessible by subject external to the TCB shall be maintained by the TCB. These labels shall be used as the basis for mandatory protection decisions. In order to import non-labelled data, the TCB shall request and receive from an authorized user the sensitivity level of the data, and all such actions shall be auditable by the TCB.

(1) Label Accuracy. Sensitivity labels shall accurately represent the sensitivity of the specific subjects or objects with which they are associated. When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported.

(2) Exportation of Labelled Information. The TCB shall designate each communication channel and I/O device as either single-level or multilevel. Any change in this designation shall be done manually and shall be auditable by the TCB. The TCB shall maintain and be able to audit any change in the sensitivity levels associated with a communication channel or I/O device.

(a) Exportation to Multilevel Devices. When TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When the TCB exports or imports an object over a multilevel communication channel, the protocol used on that channel shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received.

(b) Exportation to Single-level Devices. Single-level I/O devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process. However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the sensitivity of information imported or exported via single-level communication channels or I/O devices.

(c) Labelling Human-Readable Output. The EDP system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning and end of all human-readable paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly represent the

sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels of the output or that properly represent the sensitivity of the information on the page. The TCB shall, by default and in an appropriate manner, mark other forms of human-readable output with sensitivity labels that properly represent the sensitivity of the output. Any override of these marking defaults shall be auditable by the TCB.

(3) Subject Sensitivity Labels. The TCB shall immediately notify a terminal user of each change in the sensitivity associated with that user during an interactive session. A terminal user shall be able to query the TCB as desired for a display of the subject's complete sensitivity label.

(4) Device Labels. The TCB shall support the assignment of minimum and maximum sensitivity to all attached physical devices. These sensitivity shall be used by the TCB to enforce constraint imposed by the physical environments in which the devices are located.

C. PARTITIONS: HIERARCHIES AND COMPARTMENTS

1. Level CP-0: Noncompliant

This level, Confidentiality/Partitions: Hierarchies and Compartments Level 0 (CP-0) is reserved for those products which have been evaluated but fail to meet the requirements of any of the Partitions requirements of confidentiality.

2. Level CP-1: Compartments

The TCB shall enforce a mandatory protection policy over all subjects and storage objects under its control (i.e., processes, files, segments, devices). These subjects and objects shall be assigned labels that designate partitions of data which can be combined in specific structures defined by the security policy as described by the TCB. These labels

shall be used as the basis for mandatory protection decisions. The protection mechanism shall be able to support multiple compartments which shall separate user workspaces into well defined, and protected areas.

3. Level CP-2: Compartmentalized Hierarchies

The TCB shall enforce a mandatory protection policy over all resources (i.e., subjects, storage objects, and I/O devices) that are directly or indirectly accessible by subjects external to the TCB. These subjects and objects shall be assigned hierarchical levels and non-hierarchical compartments, and these shall be used as the basis for mandatory protection decisions. The TCB shall be able to support multiple hierarchical levels each capable of containing multiple, non-hierarchical components.

4. Level CP-3: Multiple Compartmentalized Hierarchies

The TCB shall enforce a mandatory protection policy over all resources (i.e., subjects, storage objects, and I/O devices) that are directly or indirectly accessible by subjects external to the TCB. These subjects and objects shall be assigned hierarchical levels and non-hierarchical compartments, and these shall be used as the basis for mandatory protection decisions. The TCB shall be able to support at least two distinct hierarchies, each of which is capable of containing multiple non-hierarchical compartments.

5. Level CP-4: Embedded Hierarchies and Compartments

The TCB shall enforce a mandatory protection policy over all resources (i.e., subjects, storage objects, and I/O devices) that are directly or indirectly accessible by subjects external to the TCB. These subjects and objects shall be assigned hierarchical levels and non-hierarchical compartments, and these shall be used as the basis for mandatory protection decisions. The TCB shall be able to support multiple hierarchical

levels each capable of containing multiple non-hierarchical components, each of which contain embedded hierarchies and compartments. The TCB shall be able to support at least three embedded levels.

D. OBJECT RE-USE

1. Level CR-0: Noncompliant

This level, Confidentiality/Object Re-Use Level 0 (CR-0) is reserved for those products which have been evaluated but fail to meet the requirements of any of the object reuse controls required by confidentiality.

2. Level CR-1: Object Re-Use

All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation of the object to a subject from the product's pool of unused storage objects. No information produced by a prior subject's action is to be available to any subject that obtain access to an object that has been released back to the system. Encrypted representations of information will only be considered as unavailable if the encryption mechanism has been specifically approved for such an application by the certification authority.

III.INTEGRITY

The Integrity Criteria for the Indonesian Navy are being developed as the loose form dual of the confidentiality criteria. The basic structure of the integrity criteria is expected to follow that of the confidentiality criteria and will be based on recent work in the area of integrity by Clark and Wilson and others. It would be helpful if any efforts by the NCSC in this area were available. The following sections contains the proposed structure of the integrity criteria.

A. DISCRETIONARY PROTECTION

Levels within this division provide for discretionary protection - at the control of the owner.

1. Level ID-0: Noncompliant

This level, Integrity/Discretionary Protection Level 0 (ID-0) is reserved for those products which have been evaluated but fail to meet the requirements of any of the Discretionary Protection required by integrity.

2. Level ID-1: Discretionary Execution Protection

An Integrity/Discretionary Protection Level 1 (ID-1) product nominally satisfies the discretionary requirements by providing separation of users and data. It incorporates some form of credible controls capable of enforcing access limitations on an individual basis.

The TCB shall define and control execution of named processes by named subjects (e.g., users, processes) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, execution control lists, etc.) shall allow users to specify and control

execution of named processes by named individuals, or defined groups of individuals, or by both, and shall provide controls to limit propagation of execution rights.

3. Level ID-2: Discretionary Execution Protection

The TCB shall define and control execution of named processes by named subjects (e.g., users, processes) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, execution lists, etc.) shall allow users to specify and control execution of named processes by named individuals, or defined groups of individuals, or by both, and shall provide controls to limit propagation of execution rights. The discretionary execution control mechanism shall, either by explicit action or by default, provide that processes are protected from unauthorized invocation. These execution controls shall be capable of including execution to the granularity of a single subject (e.g., user, process, etc.). Invocation privileges shall only be assigned by authorized users.

4. Level ID-3: Discretionary Execution Protection

The TCB shall define and control execution of named processes by named subjects (e.g., users, processes) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, execution lists, etc.) shall allow users to specify and control execution of named processes by named individuals, or defined groups of individuals, or by both, and shall provide controls to limit propagation of execution rights. These execution controls shall be capable of specifying, for each named process, a list of named subjects and a list of groups of named subjects with invocation privileges for a named process. Furthermore, for each such named process, it shall be possible to specify a list of groups of named subjects for which no invocation privilege to a named process is to be given.

B. MANDATORY PROTECTION

1. Level IM-0: Noncompliant

This level is reserved for those products that have been evaluated but fail to meet the requirements for a higher level.

2. Level IM-1: Mandatory Execution Protection

The TCB shall enforce a mandatory execution control policy over all processes. These processes shall be assigned integrity labels and the labels shall be used as the basis for mandatory execution control decisions. The TCB shall be able to support N or more integrity domains. Requirements for invocation privileges shall be specified by an authorized subject external to TCB. Identification and authentication data shall be used by the TCB to authenticate the identify of a user invoking a process and to ensure that the integrity attributes of the subjects external to the TCB that are invoked on behalf of the individual user are consistent with the integrity attributes of that user (Note:"are consistent with" must be defined).

3. Level IM-2: Mandatory Execution Protection

The TCB shall enforce a mandatory execution control policy over all processes that can be directly or indirectly invoked by subjects external to the TCB. Requirements for direct or indirect invocation of any process by any subject external to the TCB shall be specified by an authorized subject external to the TCB. Identification and authentication data shall be used by the TCB to authenticate the identify of a user invoking a process and to ensure that the integrity attributes of the subjects external to the TCB that are invoked on behalf of the individual user are consistent with the integrity attributes of that user (Note:"are consistent with" must be defined).

C. SEPARATION OF DUTIES

Products in this division must include mechanisms by which to separate and define various functions within the system. The granularity defined by the system relates directly to the level which it attains.

1. Level IS-0: Noncompliant

This level, Separation of Duties Level 0 (IS-0) is reserved for those products which have been evaluated but fail to meet the requirements of any of the separation of duties required by the integrity criteria.

2. Level IS-1: Basic Separation

The system is broken down into two domains: User and System Administrator. This form of separation is considered minimal and may not be sufficient for more secure systems. It must be shown that two domains are separate and that a user can not become system administrator except from specific, verified locations (i.e., system console).

3. Level IS-2: Administrative Separation

The system separates users by type: System Administrator, Operator, User, etc. Each user has specific tasks which are attached to the user type. Each user type is unique and non-overlapping.

4. Level IS-3: Administrative Compartmentalization

The system separates users by type (System Administrator, Operator, User, etc.) but each is restricted to the form of on-line interaction. Some administrative tasks are mutually exclusive while others can not be done on a live system. Each user type is mapped out and defined in terms of interaction with the other. Some administrative duties must be done in two-man rule, requiring two, distinct user types to be active for a specific duty to

be accomplished. Certain duties shall require that the system be unavailable to normal users, such as system recovery and backup.

5. Level IS-4: Logical Separation

The system is broken down into domains corresponding to logical uses of the system. Each domain is non-overlapping and self-contained (compartmentalized). Users from one domain can not transfer over or enter the domains of other users.

IV. AVAILABILITY

(Not Yet Complete)

V.ACCOUNTABILITY

The accountability criteria are drawn directly from the TCSEC. Consideration will be given to developing them further based on requirements to more completely support integrity issues.

A. IDENTIFICATION AND AUTHENTICATION

1. Level WI-0: Noncompliant

This level, Accountability/Identification And Authentication Level 0 (WI-0) is reserved for those products which have been evaluated under the Accountability/ Identification And Authentication Criteria but have failed to meet the requirements for a higher evaluation class.

2. Level WI-1: Discretionary Security Protection

User shall be required to identify themselves to the TCB before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanisms to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user.

3. Level WI-2: Controlled Access Protection

User shall be required to identify themselves to the TCB before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanisms to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify

each individual EDP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

4. Level WI-3: Labelled Security Protection

User shall be required to identify themselves to the TCB before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall maintain authentication data that includes information for verifying the identity of individual users (e.g. passwords) as well as information for determining the clearance and authorizations of individual users. This data shall be used by the TCB to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual EDP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

B. AUDIT

1. Level WA-0: Noncompliant

This level, Accountability/Audit Level 0 (WA-0) is reserved for those products which have been evaluated under the Accountability/Audit Criteria but have failed to meet the requirements for a higher evaluation class.

2. Level WA-1: Controlled Access Protection

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record, at minimum, the following type of events: user of identification and authentication mechanisms, introduction of objects into

a user's address space (e.g., file open, program initiation), deletion of objects, actions taken by computer operators and system administrator and/or system security officers, and other security relevant events. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/ authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The EDP system administrator shall be able to selectively audit the action of any one or more users based on individual identity.

3. Level WA-2: Labelled Security Protection

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record, at minimum, the following type of events: user of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, actions taken by computer operators and system administrator and/or system security officers, and other security relevant events. The TCB shall also be able to audit any override of human-readable output markings. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/ authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object and the object's sensitivity. The EDP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity and/or object sensitivity.

4. Level WA-3: Structured Protection

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record, at minimum, the following type of events: user of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, actions taken by computer operators and system administrator and/or system security officers, and other security relevant events. The TCB shall also be able to audit any override of human-readable output markings. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/ authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object and the object's sensitivity. The EDP system administrator shall be able to selectively audit the action of any one or more users based on individual identity and/or object sensitivity. The TCB shall be able to audit the identified events that may be used in the exploitation of covert storage channels.

5. Level WA-4: Security Domains

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record, at minimum, the following type of events: user of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, actions taken

by computer operators and system administrator and/or system security officers, and other security relevant events. The TCB shall also be able to audit any override of human-readable output markings. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/ authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object and the object's sensitivity. The EDP system administrator shall be able to selectively audit the action of any one or more users based on individual identity and/or object sensitivity. The EDP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity and/or object security level. The TCB shall be able to audit the identified events that may be used in the exploitation of covert storage channels. The TCB shall contain a mechanism that is able to monitor the occurrence or accumulation of security auditable events that may indicate an imminent violation of security policy. This mechanism shall be able to immediately notify the security administrator when threshold are exceeded and, if the occurrence or accumulation of these security relevant events continues, the system shall take the least disruptive action to terminate the event.

C. TRUSTED PATH

1. Level WT-0: Noncompliant

This level, Accountability/Trusted Path Level 0 (WT-0) is reserved for those products that have been evaluated under the Accountability/Trusted Path Criteria but have failed to meet the requirements for a higher evaluation class.

2. Level WT-1: Structured Protection

The TCB shall support a trusted communication path between itself and user for initial login and authentication. Communications via this path shall be initiated exclusively by a user.

3. Level WT-2: Security Domains

The TCB shall support a trusted communication path between itself and user for use when a positive TCB-to-user connection is required (e.g., login, change subject sensitivity). Communications via this trusted path shall be activated exclusively by a user or the TCB and shall be logically isolated and unmistakably distinguishable from other paths.

VI. ASSURANCE

The assurance criteria are used to establish the degree to which evidential support and subsequent reasoning exists about the degree to which the chosen product mechanisms and design will, throughout the life of a product, support the specified product security policy.

The initial draft of the assurance criteria directly extracted from the TCSEC.

Additional factors (such as the development environment, hardware design control, intrusion detection) will be considered for further specification of the criteria.

A. OPERATIONAL TRUST

- **Product Integrity**

For all levels of operational trust, hardware and/or software features shall provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

1. Level TO-0: Noncompliant

This level, Assurance/Operational Trust Level 0 (TO-0), is reserved for those products which have been evaluated but fail to meet the requirements of any of the operational trust mechanisms required by assurance.

2. Level TO-1: Vendor Assured

a. Product Architecture

The TCB shall maintain a domain for its own execution that protects it from external interference of tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the EDP product.

3. Level TO-2: Independently Tested

a. Product Architecture

The TCB shall maintain a domain for its own execution that protects it from external interference of tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the EDP product. The TCB shall isolate the resources to be protected so that they are subject to the protection and auditing requirements.

4. Level TO-3: independently Assured

a. Product Architecture

The TCB shall maintain a domain for its own execution that protects it from external interference of tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the EDP product. The TCB shall maintain process isolation through the provision of distinct address space under its control. The TCB shall isolate the resources to be protected so that they are subject to the protection and auditing requirements.

5. Level TO-4: Structured Design

a. Product Architecture

The TCB shall maintain a domain for its own execution that protects it from external interference of tampering (e.g., by modification of its code or data structures). The TCB shall maintain process isolation through the provision of distinct address spaces under this control. The TCB shall be internally structured into well-defined largely independent modules. It shall make effective use of available hardware to separate those elements that are protection-critical from those that are not. The TCB modules shall be designed such that the principle of least privilege is enforced. Features in hardware, such as segmentation,

shall be used to support logically distinct storage objects with separate attributes (namely: readable, writeable). The user interface to the TCB shall be completely defined and all elements of the TCB identified.

b. Covert Channel Analysis

The product developer shall conduct a thorough search for covert storage channels and make a determination (either by actual measurement or by engineering estimation) of the maximum bandwidth of each identified channel.

c. Trusted Facility Management

The TCB shall support separate operator and system administrator functions.

6. Level TO-5: Rigorous Design/Security Domains

a. Product Architecture

The TCB shall maintain a domain for its own execution that protects it from external interference of tampering (e.g., by modification of its code or data structures). The TCB shall maintain process isolation through the provision of distinct address spaces under this control. The TCB shall be internally structured into well-defined largely independent modules. It shall make effective use of available hardware to separate those elements that are protection-critical from those that are not. The TCB modules shall be designed such that the principle of least privilege is enforced. Features in hardware, such as segmentation, shall be used to support logically distinct storage objects with separate attributes (namely: readable, writeable). The user interface to the TCB shall be completely defined and all elements of the TCB identified. The TCB shall be designed and structured to use a complete, conceptually simple protection mechanism with precisely defined semantics. This mechanism shall play a central role in enforcing the internal structuring of the TCB and the product. The TCB shall incorporate significant use of layering, abstraction and data

hiding. Significant product engineering shall be directed toward minimizing the complexity of the TCB and excluding from the TCB modules that are no protection-critical.

b. Covert Channel Analysis

The product developer shall conduct a thorough search for covert storage channels and make a determination (either by actual measurement or by engineering estimation) of the maximum bandwidth of each identified channel.

c. Trusted Facility Management

The TCB shall support separate operator and system administrator functions. The functions performed in the role of a security administrator shall be defined. The EDP product administrative personnel shall only be able to perform security administrator functions after taking a distinct auditable action to assume the security administrator role on the EDP product. Non-security functions that can be performed in the security administration role shall be limited strictly to those essential to performing the security role effectively.

d. Trusted Recovery

Procedures and/or mechanisms shall be provided to assure that, after an EDP product failure of other discontinuity, recovery without a protection compromise is obtained.

7. Level TO-6: Formal Design

a. Product Architecture

The TCB shall maintain a domain for its own execution that protects it from external interference of tampering (e.g., by modification of its code or data structures). The TCB shall maintain process isolation through the provision of distinct address spaces under this control. The TCB shall be internally structured into well-defined largely independent

modules. It shall make effective use of available hardware to separate those elements that are protection-critical from those that are not. The TCB modules shall be designed such that the principle of least privilege is enforced. Features in hardware, such as segmentation, shall be used to support logically distinct storage objects with separate attributes (namely: readable, writeable). The user interface to the TCB shall be completely defined and all elements of the TCB identified. The TCB shall be designed and structured to use a complete, conceptually simple protection mechanism with precisely defined semantics. This mechanism shall play a central role in enforcing the internal structuring of the TCB and the product. The TCB shall incorporate significant use of layering, abstraction and data hiding. Significant product engineering shall be directed toward minimizing the complexity of the TCB and excluding from the TCB modules that are no protection-critical.

b. Covert Channel Analysis

The product developer shall conduct a thorough search for covert storage channels and make a determination (either by actual measurement or by engineering estimation) of the maximum bandwidth of each identified channel. Formal methods shall be use in the analysis.

c. Trusted Facility Management

The TCB shall support separate operator and system administrator functions. The functions performed in the role of a security administrator shall be identified. The EDP product administrative personnel shall only be able to perform security administrator functions after taking a distinct auditable action to assume the security administrator role on the EDP product. Non-security functions that can be performed in the security administration role shall be limited strictly to those essential to performing the security role effectively.

d. Trusted Recovery

Procedures and/or mechanisms shall be provided to assure that, after an EDP product failure of other discontinuity, recovery without a protection compromise is obtained.

B. LIFE CYCLE TRUST

- **Configuration Management (levels 1 - 5)**

During development and maintenance of any TCB, a configuration management system shall be in place that maintains control of changes to the descriptive top-level specification, other design data, implementation documentation, source code, the running version of the object code, and test fixtures and documentation. The configuration management product shall assure a consistent mapping among all documentation and code associated with the current version of the TCB. Tools shall be provided for generation of a new version of the TCB from source code. Also available shall be tools for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB.

1. Level TL-0: Noncompliant

This level, Assurance/Life Cycle Trust Level 0 (TO-0), is reserved for those products which have been evaluated but fail to meet the requirements of any of the life cycle trust mechanisms required by assurance.

2. Level TL-1: Vendor Assured

a. Security Testing

The security mechanisms of the EDP product shall be tested and found to work as claimed in the product documentation. Testing shall be done to assure that there

are no obvious ways for an unauthorized user to by pass or otherwise defeat the security protection mechanisms of the TCB.

3. Level TL-2: Independently Tested

a. Security Testing

The security mechanisms of the EDP product shall be tested and found to work as claimed in the product documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to by pass or otherwise defeat the security protection mechanisms of the TCB. Testing shall also include a search for obvious flaws that would allow violation of resource isolation, or that would permit unauthorized access to the audit or authentication data.

4. Level TL-3: Independently Assured

a. Security Testing

The security mechanisms of the EDP product shall be tested and found to work as claimed in the product documentation. A team of individuals who thoroughly understand the specific implementation of the TCB shall subject its design documentation, source code, and object code to thorough testing. Their objectives shall be: to uncover all design and implementation flaws that would permit a subject external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB; as well as to assure that no subject (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users. All discovered flaws shall be removed or neutralized and the TCB retested to demonstrate that they have been eliminated and that new flaws have not been introduced.

b. Design Specification and Verification

An informal or formal model of the security policy supported by the TCB shall be maintained over the life cycle of the EDP product and demonstrated to be consisted with its axioms.

5. Level TL-4: Structured Design

a. Security Testing

The security mechanisms of the EDP product shall be tested and found to work as claimed in the product documentation. A team of individuals who thoroughly understand the specific implementation of the TCB shall subject its design documentation, source code, and object code to thorough analysis and testing. Their objectives shall be: to uncover all design and implementation flaws that would permit a subject external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB; as well as to assure that no subject (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users. The TCB shall be found relatively resistant to penetration. All discovered flaws shall be corrected and the TCB retested to demonstrate that they have been eliminated and that new flaws have not been introduced. Testing shall demonstrate that the TCB implementation is consistent with the descriptive top-level specification.

b. Design Specification and Verification

A formal model of the security policy supported by the TCB shall be maintained over the life cycle of the EDP product that is proven consistent with its axioms. A descriptive top-level specification (DTLS) of the TCB shall be maintained that

completely and accurately describes the TCB in terms of exceptions, error messages, and effects. It shall be shown to be an accurate description of the TCB interface.

6. Level TL-5: Rigorous Design/Security Domains

a. Security Testing

The security mechanisms of the EDP product shall be tested and found to work as claimed in the product documentation. A team of individuals who thoroughly understand the specific implementation of the TCB shall subject its design documentation, source code, and object code to thorough analysis and testing. Their objectives shall be: to uncover all design and implementation flaws that would permit a subject external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB; as well as to assure that no subject (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users. The TCB shall be found relatively resistant to penetration. All discovered flaws shall be corrected and the TCB retested to demonstrate that they have been eliminated and that new flaws have not been introduced. Testing shall demonstrate that the TCB implementation is consistent with the descriptive top-level specification. No design flaws and no more than a few correctable implementation flaws may be found during testing and there shall be reasonable confidence that few remain.

b. Design Specification and Verification

A formal model of the security policy supported by the TCB shall be maintained over the life cycle of the EDP product that is proven consistent with its axioms. A descriptive top-level specification (DTLS) of the TCB shall be maintained that completely and accurately describes the TCB in terms of exceptions, error messages, and

effects. It shall be shown to be an accurate description of the TCB interface. A convincing argument shall be given that the DTLS is consistent with the model.

7. Level TL-6: Formal Design

a. Security Testing

The security mechanisms of the EDP product shall be tested and found to work as claimed in the product documentation. A team of individuals who thoroughly understand the specific implementation of the TCB shall subject its design documentation, source code, and object code to thorough analysis and testing. Their objectives shall be: to uncover all design and implementation flaws that would permit a subject external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB; as well as to assure that no subject (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users. The TCB shall be found relatively resistant to penetration. All discovered flaws shall be corrected and the TCB retested to demonstrate that they have been eliminated and that new flaws have not been introduced. Testing shall demonstrate that the TCB implementation is consistent with the descriptive top-level specification. No design flaws and no more than a few correctable implementation flaws may be found during testing and there shall be reasonable confidence that few remain. Manual or other mapping of the FTLS to the source code may form a basis for penetration testing.

b. Design Specification and Verification

A formal model of the security policy supported by the TCB shall be maintained over the life cycle of the EDP product that is proven consistent with its axioms. A descriptive top-level specification (DTLS) of the TCB shall be maintained that

completely and accurately describes the TCB in terms of exceptions, error messages, and effects. A formal top-level specification (FTLS) of the TCB shall be maintained that accurately describes the TCB in terms of exceptions, error messages, and effects. The DTLS and FTLS shall include those components of the TCB that are implemented as hardware and/or firmware if their properties are visible at the TCB interface. The FTLS shall be shown to be an accurate description of the TCB interface. A convincing argument shall be given that the DTLS is consistent with the model and a combination of formal and informal techniques shall be used to show that the FTLS is consistent with the model. This verification evidence shall be consistent with that provided within the state-of-the-art of the particular Indonesian Navy-endorsed formal specification and verification system used.A mapping (manual otherwise) of the FTLS to the TCB source shall be performed to provide evidence of correct implementation.

c. *Configuration Management (Level 6 Additional Requirements)*

This section supercedes the configuration management requirements of level TL-1 to TL-5 for level TL-6 only.

During the entire life-cycle, i.e., during the design, development, and maintenance of the TCB, a configuration management system shall be in place for all security-relevant hardware, firmware, software that maintains control of changes to the formal model, the descriptive and formal top-level specifications, other design data, implementation documentation, source code, the running version of the object code, and test fixtures and documentation. The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB. Tools shall be provided for generation of a new version of the TCB from source code. Also available shall be tools, maintained under strict configuration control, for comparing a newly generated version with the previous TCB version in order to ascertain

that only the intended changes have been made in the code that will actually be used as the new version of TCB. A combination of technical, physical, and procedural safeguards shall be used to protect from an unauthorized modification or destruction the master copy or copies of all material used to generate the TCB.

d. Trusted Distribution

A trusted EDP product control and distribution facility shall be provided for maintaining the integrity of the mapping between the master data describing the current version of the TCB and the on-site master copy of the code for the current version. Procedures (e.g., site security acceptance testing) shall exist for assuring that the TCB software, firmware, and hardware updates distributed to a customer are exactly as specified by the master copies.

C. DOCUMENTATION

1. Level TD-0: Noncompliant

This level, Assurance/Documentation Level 0 (TD-0), is reserved for those products which have been evaluated but fail to meet the requirements of any of the documentation required by assurance.

2. Level TD-1: Vendor Assured

a. Documentation

(1) Security Feature User's Guide. A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

(2) Trusted Facility Manual. A manual addressed to the EDP product administrator shall present cautions about functions and privileges that should be controlled when running a secure facility.

(3) Test Documentation. The product developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and result of the security mechanisms' functional testing.

(4) Design Documentation. Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

3. Level TD-2: Independently Tested

a. Documentation

(1) Security Feature User's Guide. A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

(2) Trusted Facility Manual. A manual addressed to the EDP product administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given.

(3) Test Documentation. The product developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and result of the security mechanisms' functional testing.

(4) Design Documentation. Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

4. Level TD-3: Independently Assured

a. Documentation

(1) Security Feature User's Guide. A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

(2) Trusted Facility Manual. A manual addressed to the EDP product administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given. The manual shall describe the operator and system administrator functions related to security, to include changing the security characteristics of a user. It shall provide guidelines on the consistent and effective use of the protection features of the product, how they interact, how to securely generate a new TCB, and facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner.

(3) Test Documentation. The product developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and result of the security mechanisms' functional testing.

(4) Design Documentation. Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the

interfaces between these modules shall be described. An informal or formal description of security policy model enforced by the TCB shall be available and an explanation provided to show that it is sufficient to enforce the security policy. The specific TCB protection mechanisms shall be identified and an explanation given to show that they satisfy the model.

5. Level TD-4: Structured Design

a. Documentation

(1) Security Feature User's Guide. A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

(2) Trusted Facility Manual. A manual addressed to the EDP product administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given. The manual shall describe the operator and system administrator functions related to security, to include changing the security characteristics of a user. It shall provide guidelines on the consistent and effective use of the protection features of the product, how they interact, how to securely generate a new TCB, and facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner. The TCB modules that contain the reference validation mechanism shall be identified. The procedures for secure generation of a new TCB from source after modification of any modules in the TCB shall be described.

(3) Test Documentation. The product developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the

security mechanisms were tested, and result of the security mechanisms' functional testing. It shall include results of testing the effectiveness of the methods used to reduce covert channel bandwidth.

(4) Design Documentation. Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. The interfaces between the TCB modules shall be described. A formal description of security policy model enforced by the TCB shall be available and proven that it is sufficient to enforce the security policy. The specific TCB protection mechanisms shall be identified and an explanation given to show that they satisfy the model. The descriptive top-level specification (DTLS) shall be shown to be an accurate description of the TCB interface. Documentation shall describe how the TCB implements the reference monitor concept and give an explanation why it is tamper resistant, cannot be bypassed, and is correctly implemented. Documentation shall describe how the TCB is structured to facilitate testing and to enforce least privilege. This documentation shall also present the results of the covert channel analysis and the trade-offs involved in restricting the channels. All auditable events that may be used in the exploitation of known covert storage channels shall be identified. The bandwidth of known covert storage channels, the use of which is not detectable by the auditing mechanisms, shall be provided.

6. Level TD-5: Rigorous Design/Security Domains

a. Documentation

(1) Security Feature User's Guide. A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

(2) Trusted Facility Manual. A manual addressed to the EDP product administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given. The manual shall describe the operator and system administrator functions related to security, to include changing the security characteristics of a user. It shall provide guidelines on the consistent and effective use of the protection features of the product, how they interact, how to securely generate a new TCB, and facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner. The TCB modules that contain the reference validation mechanism shall be identified. The procedures for secure generation of a new TCB from source after modification of any modules in the TCB shall be described. It shall include the procedures to ensure that the product is initially started in a secure manner. Procedures shall also be included to resume secure product operation after any lapse in product operation.

(3) Test Documentation. The product developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and result of the security mechanisms' functional testing. It shall include results of testing the effectiveness of the methods used to reduce covert channel bandwidth.

(4) Design Documentation. Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. The interfaces between the TCB modules shall be described. A formal description of security policy model enforced by the TCB shall be available and proven that it is sufficient to enforce the security policy. The specific TCB protection mechanisms shall be identified and an explanation given to show that they

satisfy the model. The descriptive top-level specification (DTLS) shall be shown to be an accurate description of the TCB interface. Documentation shall describe how the TCB implements the reference monitor concept and give an explanation why it is tamper resistant, cannot be bypassed, and is correctly implemented. The TCB implementation (i.e., in hardware, firmware and software) shall be informally shown to be consistent with the DTLS. The elements of the DTLS shall be shown, using informal techniques, to correspond to the elements of the TCB. Documentation shall describe how the TCB is structured to facilitate testing and to enforce least privilege. This documentation shall also present the results of the covert channel analysis and the trade-offs involved in restricting the channels. All auditable events that may be used in the exploitation of known covert storage channels shall be identified. The bandwidth of known covert storage channels, the use of which is not detectable by the auditing mechanisms, shall be provided.

7. Level TD-6: Formal Design

a. Documentation

(1) Security Feature User's Guide. A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

(2) Trusted Facility Manual. A manual addressed to the EDP product administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given. The manual shall describe the operator and system administrator functions related to security, to include changing the security characteristics of a user. It shall provide guidelines on the consistent and effective use of the protection features of the product, how

they interact, how to securely generate a new TCB, and facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner. The TCB modules that contain the reference validation mechanism shall be identified. The procedures for secure generation of a new TCB from source after modification of any modules in the TCB shall be described. It shall include the procedures to ensure that the product is initially started in a secure manner. Procedures shall also be included to resume secure product operation after any lapse in product operation.

(3) Test Documentation. The product developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and result of the security mechanisms' functional testing. It shall include results of testing the effectiveness of the methods used to reduce covert channel. The results of the mapping between the formal top-level specification and the TCB source code shall be given.

(4) Design Documentation. Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. The interfaces between the TCB modules shall be described. A formal description of security policy model enforced by the TCB shall be available and proven that it is sufficient to enforce the security policy. The specific TCB protection mechanisms shall be identified and an explanation given to show that they satisfy the model. The descriptive top-level specification (DTLS) shall be shown to be an accurate description of the TCB interface. Documentation shall describe how the TCB implements the reference monitor concept and give an explanation why it is tamper resistant, cannot be bypassed, and is correctly implemented. The TCB implementation (i.e., in hardware, firmware and software) shall be informally shown to be consistent with the formal top-level specification (FTLS). The elements of the FTLS shall be shown, using

informal techniques, to correspond to the elements of the TCB. Documentation shall describe how the TCB is structured to facilitate testing and to enforce least privilege. This documentation shall also present the results of the covert channel analysis and the trade-offs involved in restricting the channels. All auditable events that may be used in the exploitation of known covert storage channels shall be identified. The bandwidth of known covert storage channels, the use of which is not detectable by the auditing mechanisms, shall be provided. Hardware, firmware, and software mechanisms not dealt with in the DTLS but strictly internal to the TCB (e.g., mapping registers, direct memory access I/O) shall be clearly described.

LIST OF REFERENCES

[BUCK57] Buckles, R.A., Ideas, *Inventions, and Patents. How to Develop and Protect Them*, John Wiley & Sons, Inc., 1957.

[CSSC91] Canadian System Security Centre Communications Security Establishment Government of Canada, *The Canadian Trusted Computer Product Evaluation Criteria version 2.1e*, 1991.

[DITT90] Dittrich, K., et.al., *Computer Security and Information Integrity*, Proceeding of the Sixth IFIP International Conference on Computer Security and Information Integrity in our Changing World IFIP/Sec '90, Espoo (Helsinki), Finland, 23 - 25 May 1990, Elsevier Science Publisher B.V, 1990.

[GREE75] Greenawalt, K., Legal Protections of Privacy, Final Report to the Office of Telecommunications Policy Executive Office of the President, for sale by Superintendent of Documents, U.S. Government Printing Office, 1975.

[HOLB91] Holbrook, P., *Site Security Handbook*, Network Working Group, July 1991.

[JOHN85] Johnson, D.G., and Snapper, J.W., *Ethical Issues in the Use of Computers*, Wadsforth Publishing Company, 1985.

[LANE85] Lane, V. P., *Security of Computer Based Information Systems*, MacMillan Education Ltd., 1985.

[MART73] Martin, J., *Security, Accuracy, and Privacy in Computer Systems*, Prentice-Hall, Inc., 1973.

[NCSC85] National Computer Security Center's Technical Guideline Program, *Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC)*, Orange book, 1985.

[PFLE89] Pfleefger, C.P., *Security in Computing*, Prentice Hall, 1989.

[RUSS91] Russel, D., and G.T. Gangemi Sr, *Computer Security Basics*, O'Reilley & Associates, Inc, 1991.

[SOGI91] Senior Officials Group - Information System Security Commission of the European Communities Directorate XIII/F, *Information Technology Security Evaluation Criteria (ITSEC)*, Department of Trade and Industry, London, June 1991.

[STON92] Stone, H.S., "Copyrights and Author Responsibilities", *IEEE Computer*, December 1992.

[WEIS92] Weisband, S.P., and Goodman, S.E., "News from the Committee on Public Policy, International Software Piracy", *IEEE Computer*, November 1992.

INITIAL DISTRIBUTION LIST

Defense Technical Information Center Cameron Station Alexandria, VA 22304-6145	2
Dudley Knox Library Code 52 Naval Postgraduate School Monterey, CA 93943-5002	2
Chairman, Code CS Computer Science Department Naval Postgraduate School Monterey, CA 93943	2
Dr. Timothy J. Shimeall Computer Science Department, Code CSSm Naval Postgraduate School Monterey, CA 93943	2
Dr. Roger Stemp Computer Science Department, Code CSSp Naval Postgraduate School Monterey, CA 93943	1
Commander Naval Computer and Telecommunication Command 4401 Massachusetts Ave., N.W. Washington, DC 20394 - 5000	1
Defense Information Systems Agency (TFEF) 3701 North Fairfax Dr. Arlington, VA 22203 - 1713	1
Commander, Naval Training Command (DANKODIKAL) Morokrembangan Surabaya Indonesia	1

Director, Naval Education (DIRDIKAL) 1
Indonesian Naval Headquarters
Cilangkap Jakarta
Indonesia

Maj. Antonius Herusutopo, IDN 2
Jl.Kalamisani 10 Ujung
Surabaya 60155
Indonesia

DUDLEY KNOX LIBRARY
NAVAL POSTGRADUATE SCHOOL
MONTEREY CA 93943-5101

GAYLORD S

AMERICAN BINDERY
6-84

DUDLEY KNOX LIBRARY
3 2768 00019264 5